

Simulacija rada IoT mreže primjenom programske podrške Cisco Packet Tracer

Arapović, Ivan

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:119:082958>

Rights / Prava: [In copyright / Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-05-20**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences -
Institutional Repository](#)



**SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI**

Ivan Arapović

**SIMULACIJA RADA IOT MREŽE PRIMJENOM PROGRAMSKE
PODRŠKE CISCO PACKET TRACER**

DIPLOMSKI RAD

Zagreb, 2021.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

**SIMULACIJA RADA IOT MREŽE PRIMJENOM
PROGRAMSKE PODRŠKE CISCO PACKET TRACER
IOT NETWORK SIMULATION USING CISCO PACKET
TRACER SOFTWARE SUPPORT**

Mentor: prof. dr. sc. Zvonko Kavran
Komentor: dr.sc. Ivan Cvitić

Student: Ivan Arapović
JMBAG: 0135238421

Zagreb, rujan 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 8. lipnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Planiranje telekomunikacijskih mreža**

DIPLOMSKI ZADATAK br. 6552

Pristupnik: **Ivan Arapović (0135238421)**
Studij: **Promet**
Smjer: **Informacijsko-komunikacijski promet**

Zadatak: **Simulacija rada IoT mreže primjenom programske podrške Cisco Packet Tracer**

Opis zadatka:

Dizajnirati IoT mrežu sa odgovarajućim klasama uređaja. Analizirati utjecaj pojedinih elemenata u mreži na sigurnost, pouzdanost i kvalitetu rada mreže.

Mentor:

Predsjednik povjerenstva za
diplomski ispit:

prof. dr. sc. Zvonko Kavran

dr. sc. Ivan Cvitić (komentor)

SAŽETAK

IoT predstavlja tehnologiju koja veoma brzo raste u svim područjima primjene, a osobito na području mreže pametne kuće. Danas su IoT uređaji sveprisutni, mnogo poslovnih i privatnih aktivnosti se obavlja pomoću ove tehnologije te su brojne i olakšane implementacijom ovog koncepta u svakodnevicu. Upotrebom pametnih uređaja i aplikacija unutar njih te s povećanim opsegom usluga te pogodnosti koje donose, IoT mreža unutar pametne kuće donijela je brojne prednosti. Naglasak je i na pouzdanosti, kvaliteti i sigurnosti ovakve vrste mreže s obzirom da je prisutna u ključnim segmentima korisnikovog života. IoT mreža povezuje mnogo uređaja, može predstavljati veliki sustav, razlikuje više arhitektura te koristi brojna softverska rješenja. Koristi i brojne komunikacijske tehnologije, kao i protokole, s obzirom da se unutar IoT mreže konstantno odvija razmjena informacija, poruka i podataka.

KLJUČNE RIJEČI: Internet of Things (IoT); pametna kuća; IoT mreža; simulacija IoT mreže

SUMMARY

IoT is a technology that is growing very fast in all areas of application, especially in the area of the smart home network. Today, IoT devices are ubiquitous, many business and private activities are performed using this technology and are numerous and facilitated by the implementation of this concept in everyday life. By using smart devices and applications within them, and with a greater range of services and the benefits they bring, the IoT network within a smart home has brought a number of benefits. The emphasis is also on the reliability, quality and security of this type of network, given that it is present in key segments of the user's life. An IoT network connects many devices, can represent a large system, distinguishes multiple architectures, and uses a number of software solutions. It also uses a number of communication technologies, as well as protocols, since information, messages and data are constantly exchanged within the IoT network.

KEY WORDS: Internet of Things (IoT), Smart home, IoT network, IoT network simulation

SADRŽAJ

1. Uvod	1
2. Razvoj koncepta IoT	3
2.1. Povijesni pregled razvoja	3
2.2. Arhitektura IoT mreže	5
2.2.1. Slojevita arhitektura koncepta IoT	6
2.2.2. Uslužno orijentirana arhitektura	7
2.2.3. Arhitektura posredničkog softvera	8
2.2.4. Ključni elementi arhitekture IoT	10
2.3. Karakteristike koncepta IoT	11
2.4. Mogućnost primjene IoT-a	12
2.4.1. Pametna kuća	12
2.4.2. Pametna industrija	14
2.5. Prednosti i nedostaci IoT-a	15
2.6. Budućnost koncepta IoT	17
3. Programska podrška za koncept IoT	20
3.1. Programska podrška za uređaje koncepta IoT	21
3.2. Programska podrška za pristupnike u konceptu IoT	22
3.3. Programska podrška za cloud i analitiku koncepta IoT	23
3.4. Programska podrška za aplikacije koncepta IoT	25
4. Podatkovni protokoli i komunikacijske tehnologije	26
4.1. Protokoli za prijenos podataka	26
4.1.1. MQTT protokol	27
4.1.2. XMPP protokol	28
4.1.3. DDS protokol	29
4.1.4. AMQP protokol	31

4.2. Komunikacijske tehnologije u primjeni	32
4.2.1. NFC	33
4.2.2. Bluetooth	33
4.2.3. Wi-Fi	34
4.2.4. RFID.....	34
4.2.5. LoRaWAN	35
4.2.6. ZigBee	35
5. Planiranje IoT mreže	37
5.1. Pregled Cisco Packet Tracer programske podrške	38
5.2. Kreiranje IoT mreže unutar pametne kuće	42
6. Simulacija IoT mreže na primjeru pametne kuće i analiza dobivenih rezultata	47
6.1. Mjerenje mrežnih performansi	47
6.2. Praćenje i mjerenje parametara unutar IoT mreže	53
6.3. Diskusija rezultata istraživanja.....	56
7. Zaključak	58
Literatura	59
Popis kratica	62
Popis slika	63
Popis tablica	65
Popis grafikona.....	66

1. Uvod

IoT mreža omogućuje povezivanje uređaja i daljinsko upravljanje i nadzor istih u raznim okruženjima. Posljednjih godina koncept IoT doživio je snažnu evoluciju i trenutno se koristi u različitim domenama kao što je pametna kuća. Mreža za kućnu automatizaciju, sastavljena od senzora, aktuatora i ostalih uređaja koji dijele resurse i međusobno su povezani, ključna je tehnologija za stvaranje pametnih kuća. Cilj ovog diplomskog rada je pružiti temeljni uvid u koncept IoT i mrežu, dizajnirajući istu i kroz primjere u standardnoj primjeni analizirati utjecaj pojedinih elemenata na sigurnost, pouzdanost i kvalitetu rada mreže. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Razvoj koncepta IoT
3. Programska podrška za koncept IoT
4. Podatkovni protokoli i komunikacijska tehnologija
5. Planiranje IoT mreže
6. Simulacija IoT mreže na primjeru pametne kuće i analiza dobivenih rezultata
7. Zaključak

U drugom poglavlju obrađuje se razvoj koncepta IoT kroz faze povijesnog razvoja te arhitektura IoT kroz različite vrste iste uz naglasak na ključne elemente. Nastavlja se sa opisivanjem glavnih karakteristika IoT mreže uz prednosti i nedostatke kroz koje se analizira sigurnost, pouzdanost i kvaliteta mreže. Također, u ovom poglavlju se obrađuje na primjerima primjena samog IoT-a.

Treće poglavlje sadrži pregled programske podrške koncepta IoT na osnovu programske podrške za uređaje IoT, pristupnika, programske podrške za cloud i analitiku te aplikacije unutar IoT mreže.

Četvrto poglavlje donosi temeljni uvid u podatkovne protokole i komunikacijske tehnologije u primjeni pomoću kojih se ostvaruje razmjena podataka i informacija u okviru IoT mreže.

U petom poglavlju navedeni su i analizirani elementi IoT mreže, osobito u okvirima alata Cisco Packet Tracer unutar kojega se odvija kasnija simulacija IoT mreže. Pregled tog alata, kao i mogućnosti te samo kreiranje IoT mreže unutar pametne kuće, što predstavlja srž ovog diplomskog rada, zaključuje ovo poglavlje.

Šesto poglavlje sastoji se od višestrukih simulacija u okviru određenih scenarija te prati funkcionalnost i ponašanje IoT mreže u konkretnim uvjetima unutar okruženja pametne kuće, pružajući tako uvid u kvalitetu, mogućnosti i pouzdanost ove vrste mreže.

2. Razvoj koncepta IoT

Pojam Internet stvari (eng. *Internet of things* – IoT) odnosi se na vrstu mreže koja povezuje bilo koji uređaj s Internetom putem protokola te koji razmjenjuje informacije (međusobno komunicira) u svrhu postizanja pametnog prepoznavanja, pozicioniranja, praćenja, nadzora i upravljanja. U ovom će se radu, uz simulaciju IoT mreže na temelju pametne kuće, napraviti pregled o tome što je IoT, koje različite tehnologije omogućuje, o njegovoj arhitekturi, karakteristikama i aplikacijama, funkcionalnom pogledu te o budućim izazovima za IoT, [1]. U posljednjih nekoliko godina IoT je postao jedna od najvažnijih tehnologija 21. stoljeća. Sada kada se mogu povezati predmeti svakodnevne uporabe (kuhinjski aparati, automobili, termostati, itd.) s internetom putem različitih uređaja, moguća je besprijekorna komunikacija između ljudi, procesa i stvari. Pomoću clouda, analitike i mobilnih tehnologija, fizičke stvari mogu dijeliti i prikupljati podatke uz minimalnu ljudsku intervenciju. Danas digitalni sustavi mogu bilježiti, pratiti i prilagođavati svaku interakciju između povezanih stvari. Fizički svijet susreće digitalni svijet te se može reći da oni međusobno surađuju, [2].

2.1. Povijesni pregled razvoja

Sam koncept povezanih uređaja datira iz 1832. godine kada je dizajniran prvi elektromagnetski telegraf. Telegraf je omogućio izravnu komunikaciju između dva stroja prijenosom električnih signala. Međutim, prava povijest IoT-a započela je izumom interneta krajem 1960-ih, koji se zatim brzo razvijao tijekom sljedećih desetljeća, [3].

Osamdesetih godina prošlog stoljeća, prvi povezani uređaj bio je automat Coca Cola smješten na Sveučilištu Carnegie Melon i njime su upravljali lokalni programeri. Integrirali su mikroprekidače u stroj i koristili rani oblik interneta kako bi provjerili drži li rashladni uređaj pića dovoljno hladna i ima li dostupnih limenki Coca Cole. Ovaj izum potaknuo je daljnja istraživanja na području i razvoj međusobno povezanih strojeva u cijelom svijetu, [3].

Devedesetih godina John Romkey je po prvi put spojio toster na internet s TCP/IP protokolom. Godinu dana kasnije, znanstvenici sa Sveučilišta u Cambridgeu došli su na ideju upotrijebiti prvi prototip web kamere za praćenje količine kave dostupne u loncu za kavu

lokalnog računalnog laboratorija. Programirali su web kameru da fotografira posudu za kavu tri puta u minuti, a zatim slike šalje na lokalna računala, dopuštajući tako svim korisnicima da vide ima li kave na raspolaganju, [3].

Jedna od najznačajnijih godina u povijesti IoT-a bila je 1999., kada je Kevin Ashton osmislio izraz "Internet stvari". On je držao prezentaciju za Procter & Gamble gdje je opisao IoT kao tehnologiju koja povezuje nekoliko uređaja pomoću RFID oznaka za upravljanje opskrbnim lancem. Posebno je upotrijebio riječ "internet" u naslovu svog izlaganja kako bi privukao pozornost publike budući da je internet u to vrijeme postajao sve zanimljiviji. Dok se njegova ideja o povezivanju uređaja temeljenih na RFID-u razlikuje od današnjeg IoT-a temeljenog na internetu, Ashtonov je napredak odigrao bitnu ulogu u povijesti ovog koncepta i sveukupnom tehnološkom razvoju.

Početkom 21. stoljeća pojam IoT-a ušao je u široku upotrebu u medijima. Zanimanje za IoT tehnologiju stalno se povećavalo, što je dovelo do prve međunarodne konferencije o Internetu stvari održane u Švicarskoj 2008., na kojoj su sudionici iz 23 zemlje razgovarali o RFID-u, bežičnim komunikacijama kratkog dometa i senzorskim mrežama. Štoviše, nekoliko velikih razvoja potaknulo je razvoj IoT-a. Jedan od njih bio je hladnjak spojen na internet koji je LG Electronics predstavio 2000. godine, omogućujući svojim korisnicima kupnju „online“ i video pozive. Još jedan bitan izum bio je mali robot u obliku zeca nazvan Nabaztag, stvoren 2005. godine, koji je mogao ispričati najnovije vijesti, vremensku prognozu i promjene na burzi. Prema Ciscu, čak je i tada broj međusobno povezanih uređaja premašio broj ljudi na Zemlji, [3].

IPv6 - protokol mrežnog sloja koji je središnji dio IoT-a javno je pokrenut 2011. godine. Od tada su međusobno povezani uređaji postali široko rasprostranjeni i uobičajeni u svakodnevnom životu. Apple, Samsung, Google, i Cisco počeli su fokusirati svoje napore na proizvodnju IoT senzora i uređaja od međusobno povezanih termostata i pametnih naočala do autonomnih vozila. IoT je tako pronašao svoj put u gotovo svim industrijama: proizvodnja, zdravstvo, transport, nafta i energija, poljoprivreda, maloprodaja i mnoge druge, [3].

Danas je IoT dosego visoku razinu razvijenosti i primjene što se može jasno vidjeti i po brojkama iz tablice 1 koje govore o broju povezanih uređaja.

Tablica 1. Broj povezanih uređaja od 2003. do 2020., [4]

Broj ljudi u svijetu	6.3 milijardi	6.8 milijardi	7.2 milijardi	7.6 milijardi
Povezanih uređaja	500 milijuna	12.5 milijardi	25 milijardi	50 milijardi
Uređaja po osobi	0.08	1.84	3.47	6.58
Godina	2003.	2010.	2015.	2020.

U prikazanom vremenskom periodu vidljiv je ogroman rast broja uređaja po osobi gdje danas, za razliku od 2003., korisnici u prosjeku posjeduju šest puta više uređaja. Spektar korištenja istih se znatno proširio u svakodnevnom životu te se danas gotovo većina aktivnosti ne može zamisliti bez njih, [3].

2.2. Arhitektura IoT mreže

IoT se odnosi na novu vrstu tehnologije u kojoj su gotovo svi uređaji povezani na mreže. Njihova suradnja može služiti za izvršavanje složenih zadataka visokog stupnja inteligencije. IoT nije jedinstvena tehnologija nego predstavlja skup različitih tehnologija koje zajedno rade. Senzori i aktuatori su uređaji koji pomažu u interakciji s fizičkim okruženjem. Podatke koji su prikupljeni senzori moraju inteligentno pohraniti i obraditi kako bi se iz toga proizveli korisni zaključci. Pojam senzor može označavati mobilni telefon, pa i mikrovalnu pećnicu, sve dok isti daju podatke o svom trenutnom stanju (unutarnjem stanju uz stanje okruženja). Aktuator predstavlja uređaj koji se koristi za promjenu okruženja, primjerice može se ponašati kao regulator temperature klima uređaja, [5].

Pohrana i obrada podataka mogu se obaviti na rubnom dijelu mreže ili na udaljenom poslužitelju. Ako postoji neka potreba za prethodnom obradom podataka, ona je moguća te se obično odvija na bilo kojem od senzora ili drugih bliskih uređaja. Obradeni podaci se zatim obično šalju na udaljeni poslužitelj. Pohrana i mogućnosti obrade također su ograničene raspoloživim resursima, koji su često vrlo ograničeni zbog ograničenja veličine, energije, snage i računalne sposobnosti, [5].

Što se tiče arhitekture IoT sustava, ključno je istaknuti da još ne postoji referentna arhitektura koja je dogovorena kao takva. No, postoje različite arhitekture od kojih će se u ovome radu izdvojiti one najčešće kako bi se ostvario bolji uvid u problematiku rada.

2.2.1. Slojevita arhitektura koncepta IoT

Najosnovnija arhitektura je troslojna arhitektura. Nastala je u ranim fazama istraživanja u ovome području i sastoji se od tri sloja: percepcijski, mrežni i aplikacijski sloj.

Sloj percepcije je fizički sloj koji sadrži senzore za otkrivanje i prikupljanje informacija iz okruženja. Mjeri određene fizičke parametre ili identificira druge pametne uređaje u okruženju. Mrežni sloj je odgovoran za povezivanje drugih pametnih uređaja, mrežnih uređaja i poslužitelja. Njegove značajke se također koriste za prijenos i obradu podataka dobivenih iz senzora. Aplikacijski sloj odgovoran je za isporuku aplikacije specifične usluge za korisnika. Definira razne aplikacije u kojima se Internet stvari mogu rasporediti. To su primjerice pametne kuće i pametni gradovi. Troslojna arhitektura definira glavnu ideju IoT-a, ali nije dovoljna za istraživanje o istome jer se istraživanje najviše temelji na širim aspektima Internet stvari. Zato postoji mnogo više slojevitih arhitektura, [5].



Slika 1. Troslojna i peteroslojna arhitektura IoT-a, [5].

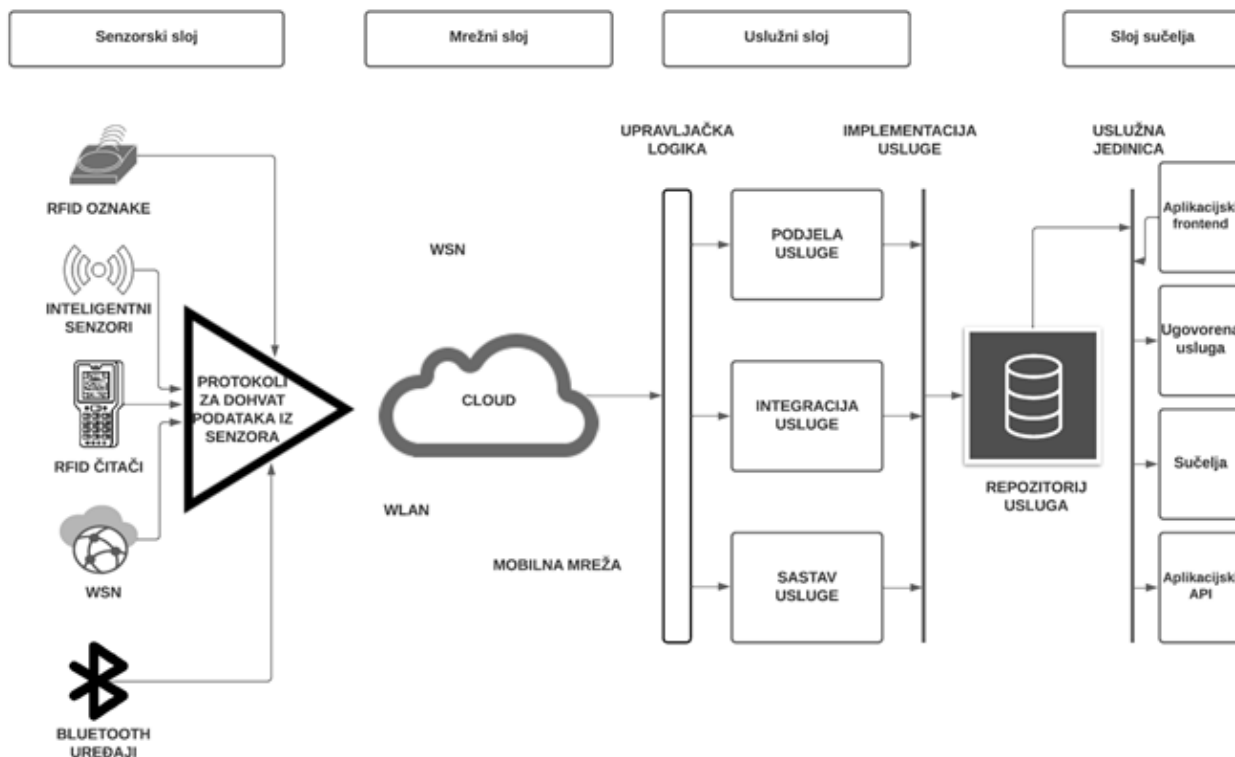
Jedna od tih je peteroslojna arhitektura, što dodatno uključuje sloj obrade i upravljački sloj. Dakle, pet slojeva predstavljaju percepcijski, transportni, aplikacijski, upravljački sloj i sloj obrade. Uloga percepcijskog i aplikacijskog sloja je kao i kod arhitekture s tri sloja. Transportni sloj prenosi podatke senzora iz percepcijskog sloja do sloja za obradu i obrnuto, putem mreža kao što su Wi-Fi, 3G, LAN, Bluetooth, RFID i NFC. Sloj za obradu poznat je i kao međusloj. Pohranjuje, analizira i obrađuje velike količine podataka koji se šalju iz transportnog sloja. Može upravljati i pružati različite vrste usluga nižim slojevima. Koristi mnoge tehnologije kao što su baze podataka, cloud i *Big Data*. Upravljački sloj upravlja cijelim IoT sustavom, uključujući aplikacije, poslovne i profitne modele te privatnost korisnika, [5].

Navedene arhitekture paralelno se mogu usporediti s procesima obrade unutar ljudskog mozga. To se odnosi na inteligenciju i sposobnost ljudskih bića kako bi mogli razmišljati, osjećati, pamtit, donositi odluke i reagirati na fizičko okruženje. Sastoji se od tri dijela: prvi je ljudski mozak, što je analogno obradi i jedinici za upravljanje podacima ili podatkovnim centrom. Drugi dio je kralježnica što je analogno distribuiranoj mreži podataka čvorova za obradu i pametnih pristupnika. Treći je mreža živaca, što odgovara mrežnim komponentama i sensorima, [5].

2.2.2. Uslužno orijentirana arhitektura

Još jedna od standardnih arhitektura u IoT-u, uslužno orijentirana arhitektura (eng. *Service Oriented Architecture - SoA*) temelji se na komponentnom modelu, koji se može dizajnirati za povezivanje različitih funkcionalnih jedinica aplikacija putem sučelja i protokola. SoA je dizajnirana za koordinaciju usluga i omogućuje ponovnu uporabu softvera i hardvera određene komponente. SoA se može lako integrirati u IoT arhitekturu, proširujući troslojnu arhitekturu, dodajući novi, uslužni, sloj između mrežnog sloja i aplikacijskog sloja, koji pruža usluge kao podršku aplikacijskom sloju. Navedeno rezultira četveroslojnom SoA-temeljenom IoT arhitekturom, u kojoj se nalaze sloj percepcije, mrežni sloj, uslužni sloj i na kraju aplikacijski sloj. Sloj usluge sastoji se od detekcije vrste usluge, sastava usluge, upravljanja uslugama i uslužnih sučelja. Otkrivanje vrste usluge koristi se za otkrivanje zahtjeva usluge, sastav usluge za interakciju s povezanim objektima i integraciju usluga radi dobivanja zahtjeva na učinkovit način, upravljanje uslugama služi za upravljanje i određivanje mehanizama povjerenja za razumijevanje zahtjeva usluga, dok se sučelja usluga koriste za

podršku interakcije između svih pruženih usluga, [6]. Na slici 2 prikazana je uslužno orijentirana arhitektura IoT-a kroz prethodno navedene slojeve.

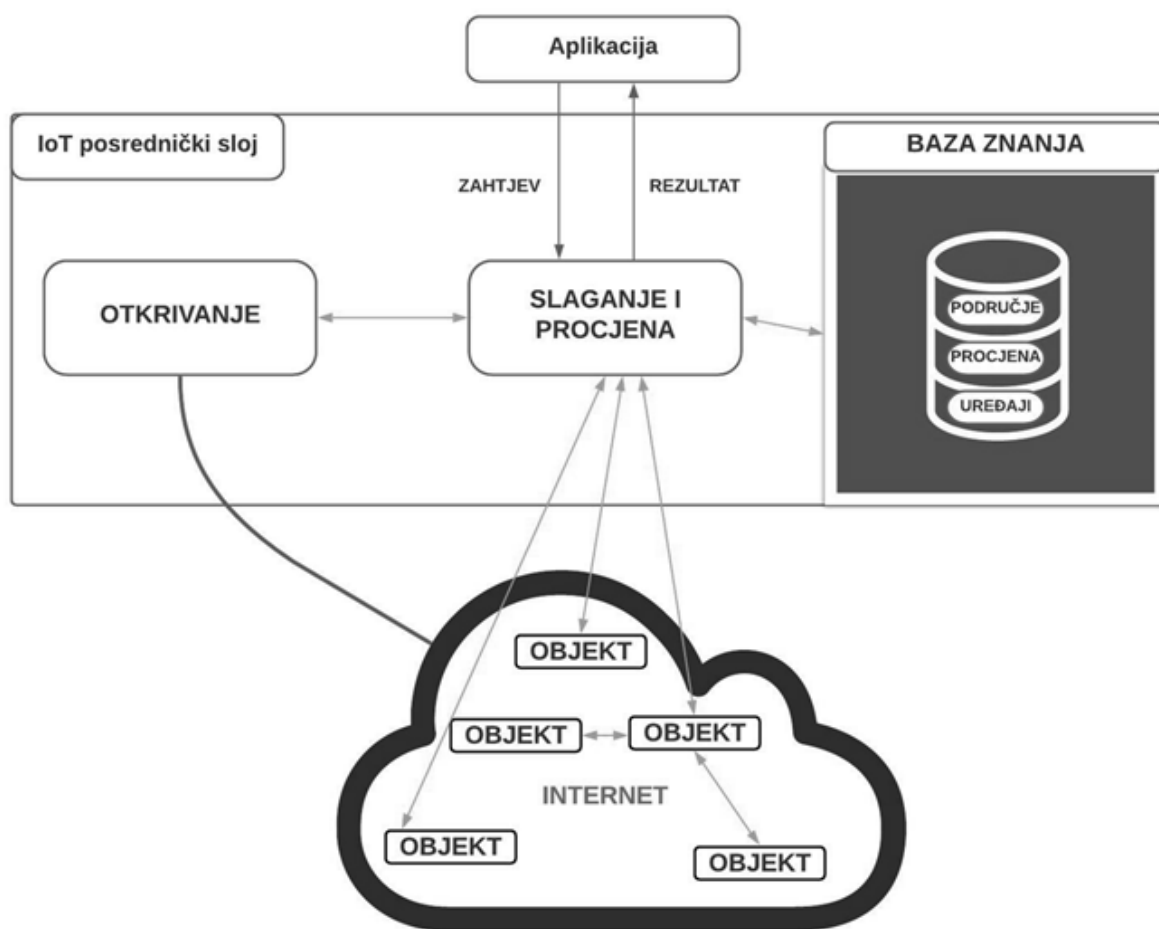


Slika 2. Uslužno orijentirana arhitektura IoT-a, [7]

2.2.3. Arhitektura posredničkog softvera

Još jedna važna i vrlo česta arhitektura u IoT-u je arhitektura posredničkog softvera. Posljednjih godina predložena arhitektura IoT -a nailazi na potrebu rješavanja mnogih čimbenika poput skalabilnosti, interoperabilnosti, pouzdanosti, kvalitete usluge, itd. U tom smislu IoT arhitekture temeljene na posredničkom softveru pomažu u povećanju učinkovitosti aplikacija. Dodani sloj posredničkog softvera djeluje kao veza između aplikacija, podataka i korisnika. Razvoj IoT -a ovisi o tehnološkom napretku i dizajnu različitih novih aplikacija i upravljačkih modela. Kako bi se omogućile postojeće i mnoge druge karakteristike, predložena je petoslojna arhitektura koja se sastoji od sloja percepcije, mrežnog sloja, sloja posredničkog softvera, aplikacijskog sloja i poslovnog sloja. Konkretno, sloj posredničkog softvera ima neke ključne funkcionalnosti, kao što je skupljanje i filtriranje primljenih

podataka s hardverskih uređaja, detekcija informacija i pružanje kontrole pristupa uređajima za aplikacije. U sloju posredničkog softvera detalji različitih tehnologija su skriveni, a standardna sučelja omogućuju razvojnim programerima da se usredotoče na razvoj aplikacija bez razmatranja kompatibilnosti između aplikacija i infrastrukture. Posrednički softver, čija je arhitektura prikazana na slici 3, posljednjih godina dobiva sve veći značaj zbog velike uloge u pojednostavljivanju razvoja novih usluga i integraciji naslijeđenih tehnologija u nove. To razvojnog programera izuzima od potrebe za značajnim poznavanjem različitog niza tehnologija koje su prethodno usvojili niži slojevi, [6].



Slika 3. Arhitektura posredničkog softvera, [8].

Prednosti posredničkog softvera su:

1. Podrška za razne aplikacije;
2. Radi na raznim operativnim sustavima i platformama;
3. Distribuirano računanje i interakcija usluga među heterogenim mrežama, uređajima i

aplikacijama;

4. Podržava standardne protokole;

5. Omogućuje standardna sučelja, pružajući prenosivost i standardne protokole za omogućavanje interoperabilnosti te čineći posrednički softver važnom ulogom u standardizaciji;

6. Pruža stabilno sučelje na visokoj razini za aplikacije, [6].

2.2.4. Ključni elementi arhitekture IoT

Bitno je istaknuti da ne postoji jedinstvena i dogovorena IoT arhitektura. Kao što se može zaključiti, razlikuje se u složenosti i broju slojeva ovisno o zahtjevu. Na primjer, referentni model koji su 2014. godine predstavili Cisco, IBM i Intel na Svjetskom forumu IoT ima čak sedam slojeva.

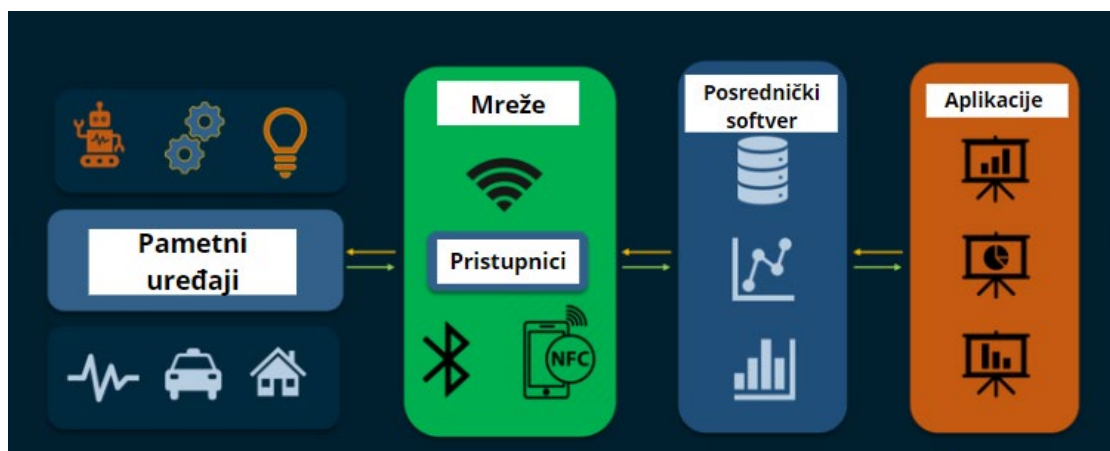
No, bez obzira na slučaj upotrebe i broj slojeva, ključni gradivni elementi uvijek su isti, a to su:

1. Pametne stvari

2. Mreže i pristupnici

3. IoT platforme koje pružaju prostor za pohranu podataka i napredne računalne mogućnosti zajedno s analitičkim mogućnostima

4. Aplikacije, omogućujući krajnjim korisnicima da imaju koristi od IoT -a i manipuliraju fizičkim svijetom.



Slika 4. Ključni gradivni elementi arhitekture IoT-a, [9].

Ključni gradivni elementi prikazani su na slici 4 gdje je na jednostavniji način prikazana okosnica svakog IoT sustava na kojem se može razviti učinkovita, višeslojna arhitektura, [9].

2.3. Karakteristike koncepta IoT

IoT se također može definirati kao dinamička mrežna infrastruktura koja ima mogućnost samokonfiguracije te se temelji na standardiziranim interoperabilnim komunikacijskim protokolima gdje fizičke i virtualne „stvari“ imaju jedinstvene identitete, fizičke attribute i virtualne osobnosti, koriste inteligentna sučelja i integrirani su u informacijsku mrežu putem Interneta pri čemu razmjenjuju podatke vezane za korisnike i njihovo okruženje. Neke od temeljnih karakteristika koncepta IoT su:

1. Međusobna povezanost - što se tiče IoT-a, gotovo sve se može povezati s globalnom informacijskom i komunikacijskom infrastrukturom.
2. Usluge povezane sa uređajima - IoT je sposoban pružiti usluge povezane s pametnim uređajima unutar ograničenja, kao što su zaštita privatnosti i semantička dosljednost između fizičkih stvari i njihovih povezanih virtualnih stvari. Kako bi se u okviru ograničenja pružale usluge povezane s pametnim uređajima, promijenit će se i tehnologije u fizičkom svijetu i svijetu informacija.
3. Heterogenost - pametni uređaji u okviru IoT-a su heterogeni jer se temelje na različitim hardverskim platformama i mrežama. Mogu komunicirati s drugim uređajima ili platformama usluga putem različitih mreža.
4. Dinamičke promjene - stanje uređaja se dinamički mijenja, kao i kontekst uređaja, uključujući lokaciju i brzinu. Štoviše, broj uređaja može se dinamički mijenjati.
5. Velika razmjernost - broj uređaja kojima je potrebno upravljati i koji međusobno komuniciraju znatno se povećavaju s vremenom, kao i upravljanje generiranim podacima i tumačenje istih za potrebe primjene.
6. Sigurnost - posebna pozornost mora se obratiti kod dizajniranja sigurnosti IoT-a zbog korisnika. To uključuje sigurnost osobnih podataka, zaštitu krajnjih točaka, mreža i podataka.
7. Povezanost - povezivanje omogućuje pristupačnost i kompatibilnost mreže. Pristupačnost postaje sve prisutnija na mreži, dok kompatibilnost pruža uobičajenu mogućnost potrošnje i proizvodnje podataka, [1].

Ovakve karakteristike konceptu IoT omogućuju međusobnu interakciju između različitih sustava te razvoj novih usluga i inteligentnih aplikacija pomoću kojih je moguće učiniti različite domene ljudskog djelovanja „pametnijima“.

2.4. Mogućnost primjene IoT-a

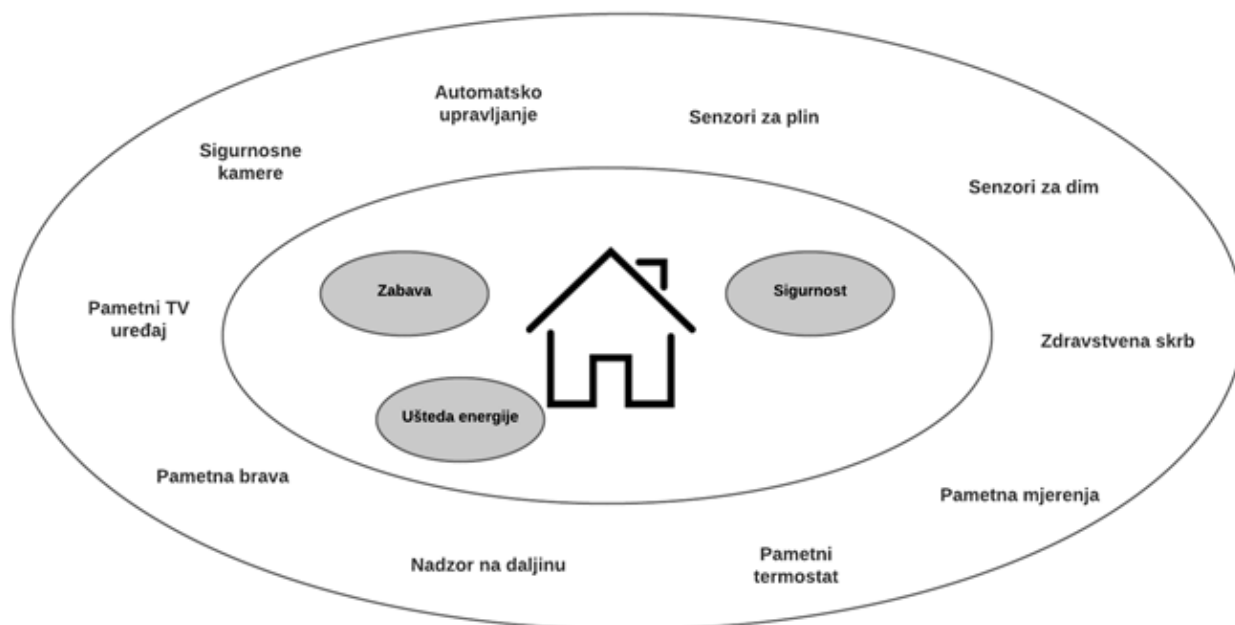
Koncept IoT-a planiran je kako bi pridonio razvoju raznih novih usluga koje su podržane platformama Interneta stvari. Glavni izazovi koji su definirani su održivi razvoj i optimalna potrošnja energije, definiranje novih tehnologija u prometu ljudi i roba, razvoj tehnologija za upravljanje poljoprivrednom proizvodnjom koja će biti prilagođena ljudskim potrebama te sigurnost Interneta. Navedeno nastoji poboljšati kvalitetu života ljudi uz istovremeno očuvanje održivog razvoja IoT koncepta i platforme temeljene na njemu koje pružaju infrastrukturu i podršku za uspješno rješavanje navedenih izazova. U nastavku će biti opisani primjeri primjene IoT koncepta s naglaskom na primjenu unutar okvira pametne kuće, čije je planiranje i simulacija u fokusu ovoga rada te kao dodatni primjer – primjena u industriji i proizvodnji.

2.4.1. Pametna kuća

Iako su pametne kuće tek zaživjele razvojem tehnologije, njihov sami koncept nije bio nepoznanica. Drugom polovicom 20. stoljeća već se počelo raditi na pametnoj kući dolaskom inovativnih kućanskih uređaja. Glavna činjenica vezana za ove inovacije je ta da znatno olakšavaju svakodnevicu jednostavnim rješenjima.

Pametna kuća podrazumijeva inteligentni sustav za nadzor i upravljanje različitim sustavima kojima je cilj poboljšati kvalitetu življenja u vlastitom domu. To je uobičajeno sustav sa centralnom mikrokontrolerskom jedinicom na koju se spajaju različiti podsustavi sa senzorima i aktuatorima. Procesi su raznoliki: uključenje i isključenje svjetla, kontrola grijanja, nadzorne kamere, pametne utičnice, senzori protiv poplave, itd. Uz signalne LED diode i LCD ekran na centralnoj jedinici, često je integrirano i daljinsko upravljanje pomoću infracrvene veze, što zahtjeva korisnikov položaj u dometu centralnoj jedinici. Pomoću daljinskog upravljača omogućuje se signalima na centralnoj jedinici slanje bežičnim putem što bitno olakšava korisniku jer nije potrebno da bude fizički prisutan u području djelovanja,

[10]. Na slici 5 prikazane su neke od funkcionalnosti pametne kuće kao što su nadzor, upravljanje temperaturom, mogućnost zdravstvene skrbi, senzori za dim, itd.



Slika 5. Funkcionalnosti pametne kuće, [5]

Prema podacima Gartnera, očekuje se da će do 2022. godine prosječno kućanstvo sadržavati više od 500 pametnih uređaja. Uzrok tome je pad cijena integriranja i nabave senzorske komunikacijske opreme i proizvoda. Također, predviđa se kako će pametne kuće u narednom desetljeću doživjeti značajan i rapidan rast u smislu opremljenosti i same primjene, [11].

Rast broja pametnih uređaja unutar kućanstava kroz povijest se razvijao ovisno o inovacijama, dostupnosti te cijeni istih. Promatrajući samo unazad par godina uređaje koji se koriste, vidljiva je velika razlika u performansama istih te opsegu mogućnosti koje pružaju. Od samih početaka, zamisao pametne kuće i povezivanja uređaja međusobno i s korisnikom putem mobilnog uređaja je da omogući uštedu vremena i financija, istodobno izvršavanje više zadataka te konstantni nadzor i upravljanje imovinom korisnika neovisno o prisutnosti. Proteklih godina uloženo je mnogo truda u procese standardizacije protokola za automatizaciju u kućanstvu. Vidnim porastom tehnologije, prisutan je i potencijal da navedeno uskoro postane i dio životnog standarda.

2.4.2. Pametna industrija

Pametna industrija predstavlja fleksibilan sustav koji može samostalno optimizirati performanse u široj mreži, samostalno se prilagoditi i učiti iz novih uvjeta u gotovo stvarnom vremenu i autonomno voditi čitave proizvodne procese. Pametna industrija može funkcionirati unutar četiri zida tvornice, ali se također može spojiti na globalnu mrežu sličnih proizvodnih sustava, pa čak i na digitalnu opskrbnu mrežu šire gledano. Pomoću tehnologije doživljava stalnu evoluciju, kontinuirano usmjerenje

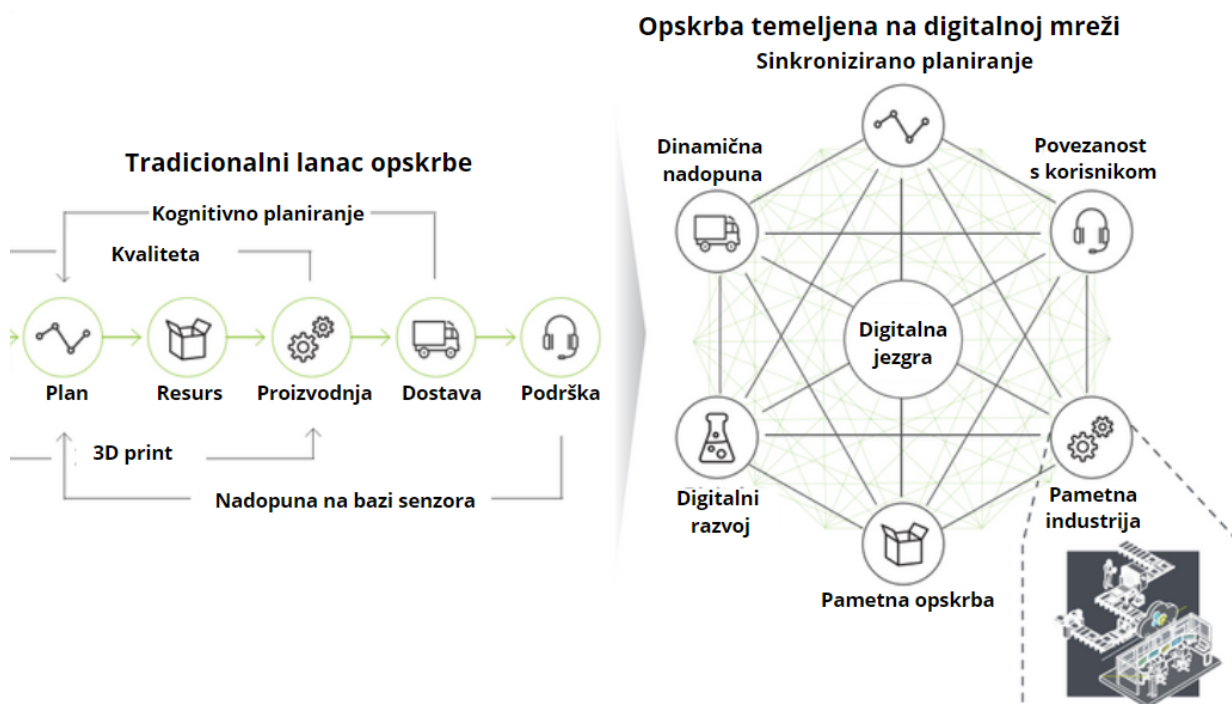
ka izgradnji i održavanju fleksibilnog sustava učenja. Glavna snaga pametne industrije leži u njenoj sposobnosti razvoja i rasta zajedno s promjenjivim potrebama tržišta - bez obzira na to mijenja li se potražnja kupaca, šire li se na nova tržišta, razvoj novih proizvoda ili usluga, održavanje, ugradnja novih procesa ili tehnologije te promjena proizvodnje u stvarnom vremenu. Zbog snažnijih računalnih i analitičkih sposobnosti, zajedno sa širim ekosustavima pametne i povezane imovine – pametna industrija može omogućiti tvrtkama da se prilagode promjenama na veoma jednostavniji i lakši način za razliku od ranije, [12].

Glavne značajke su povezanost, optimizacija, transparentnost, proaktivnost i okretnost. Svaka od ovih značajki može odigrati ulogu u omogućavanju boljih odluka u poslovanju i može pomoći organizacijama da poboljšaju proces proizvodnje. Pametna industrija zahtijeva temeljne procese i materijale koje treba povezati za generiranje podataka potrebnih za donošenje odluka u stvarnom vremenu. Unutar pametne industrije su ugrađeni uređaji s pametnim senzorima kako bi sustavi mogli neprestano povlačiti skupove podataka iz novih i tradicionalnih izvora, osiguravajući da se podaci stalno ažuriraju i odražavaju trenutne uvjete. Integracija podataka iz operacija i poslovnih sustava, kao i od dobavljača i korisnika, omogućuje cjelovit pregled procesa opskrbnog lanca, povećavajući ukupnu učinkovitost opskrbe mreže. Optimizirana pametna industrija omogućuje rad uz minimalnu ljudsku intervenciju i visoku pouzdanost. Automatski tijekovi rada, sinkronizacija imovine, poboljšano praćenje i zakazivanje te optimizirana potrošnja energije može povećati doprinos, vrijeme neprekidnog rada i kvalitete, kao i smanjiti troškove i otpad, [12].

Unutar pametne industrije podaci su transparentni zbog vizualizacije podataka u stvarnom vremenu koji mogu transformirati podatke snimljene iz procesa i na terenu ili još uvijek u proizvodnji i pretvoriti ih u one pogodne za uvid. U proaktivnom sustavu zaposlenici i sustavi mogu predvidjeti i djelovati prije nego što se pojave problemi ili izazovi te jednostavno

reagirati na njih nakon što se pojave.

Ova značajka može uključivati identificiranje anomalija, opskrbu i nadopunjavanje zaliha, identificiranje i prediktivno rješavanje pitanja kvalitete te praćenje brige o sigurnosti i održavanju.



Slika 6. Prijelaz s tradicionalnog lanca opskrbe na digitalnu mrežu opskrbe, [12]

Napredne pametne tvornice također mogu samostalno konfigurirati opremu i protok materijala, ovisno o proizvodu koji se proizvodi i promjenama rasporeda te zatim vidjeti stvarni utjecaj tih promjena kroz vrijeme. Ove značajke proizvođačima omogućuju veću vidljivost njihove imovine i sustava i omogućuju im bolje snalaženje u nekim izazovima s kojima se više suočavaju tradicionalne industrijske strukture. Slika 6 najbolje opisuje sve navedeno kroz prikaz prijelaza s tradicionalnog lanca opskrbe i karakteristika istoga na onaj temeljen na digitalnoj mreži uz sve funkcionalnosti međusobno povezane digitalnom jezgrom u jedinstvenu i funkcionalnu cjelinu.

2.5. Prednosti i nedostaci IoT-a

IoT se razvija velikom brzinom i sve je širi spektar područja u kojih se implementira. To podrazumijeva brojne koristi i prednosti po korisnike, ali i potencijalne nedostatke koje još treba nadograditi.

Prednosti se očituju najviše u olakšanje korisnikove svakodnevice, automatizaciju procesa unutar područja primjene kao što je pametna kuća i slično, poboljšanje poslovnih mogućnosti, organiziranost, povećanu kontrolu i nadzor te veću povezanost uređaja što uzrokuje i širi spektar funkcionalnosti.

Prednosti bi se prvenstveno odnosile na:

1. Komunikaciju između uređaja, na temelju koje fizički uređaji mogu ostati povezani.
2. Automatizaciju i upravljanje - bez ljudskog sudjelovanja strojevi se automatiziraju, tj. kontroliraju i obrađuju ogromne količine informacija, što dovodi do bržeg i pravovremenog rezultata.
3. Uštedu vremena i smanjenje troškova, budući da IoT koristi pametne senzore za praćenje različitih aktivnosti u svakodnevnom životu.
4. Bolju kvalitetu života - aplikacije temeljene na IoT -u omogućuju komfornost, organiziranost i lakše funkcioniranje.
5. Nove poslovne mogućnosti - povećava gospodarski rast i nova radna mjesta.
6. Ekološku osviještenost štedeći prirodne resurse, [13].

Kao i svaka tehnologija, IoT unatoč brzom napretku, sadrži nedostatke, a ponajviše one sigurnosne. Nadalje, nedostaci se mogu pronaći i unutar same infrastrukture, same složenosti takvog sustava i sl.

Nedostaci se ponajviše očituju u:

1. Kompatibilnosti iz razloga što trenutno ne postoji međunarodni standard kompatibilnosti označavanja i praćenja opreme.
2. Složenosti - IoT predstavlja raznoliku i složenu mrežu. Svaki kvar ili greške u softveru ili hardveru imat će određene posljedice.
3. Privatnosti i sigurnosti – potencijalna opasnost od neovlaštenog upada i nadgledanja privatnih podataka.
4. Složenosti softvera, budući da softverski sustavi u pametnim uređajima rade s minimalnim resursima te postoji potreba za infrastrukturnim rješenjem.
5. Toleranciji na greške - u IoT-u su pametni uređaji dinamični i brzi. Mreža stoga mora funkcionirati ispravno automatski, kako bi se prilagodili promijenjenim uvjetima, što znači da

moraju biti strukturirani za toleranciju grešaka i robustni.

6. Energetski optimiziranim rješenjima - mreža se sastoji od mnogih međusobno povezanih uređaja koji zahtijevaju visoku energiju za održavanje mreže aktivnom, što znači da je optimizacija energije jedan od bitnijih zadataka za IoT, [13].

S obzirom na navedeno, očito je kako koncept IoT donosi brojne nove mogućnosti, što sa sobom uzrokuje i potencijalne opasnosti po korisnika. Stoga se očekuje od takvog sustava da bude još razvijeniji, pouzdaniji i sigurniji u budućoj primjeni.

2.6. Budućnost koncepta IoT

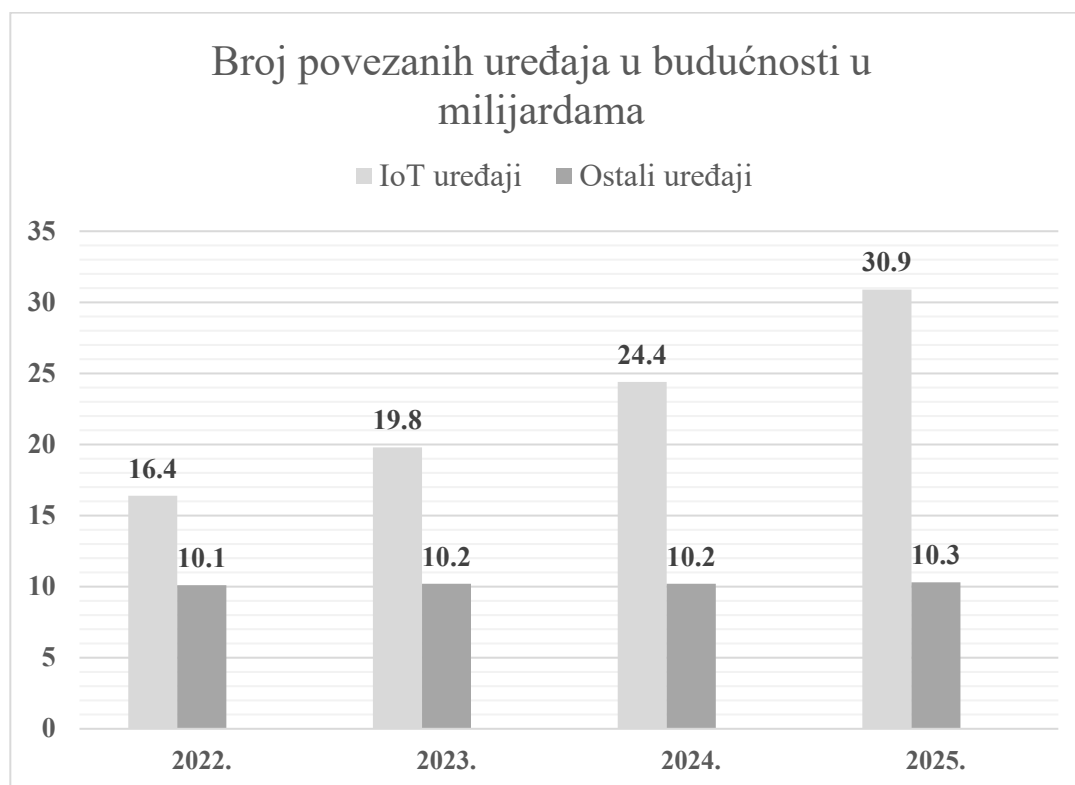
S obzirom na brzi tempo razvoja, IoT bi uskoro trebao biti vodeća tehnologija kad se govori o zastupljenosti. Sve što se može povezati bit će povezano, čime će se formirati sveobuhvatni digitalni sustav u kojem svi uređaji komuniciraju s ljudima i obrnuto. Nekoliko ključnih čimbenika koji potiču brzo širenje IoT-a su povećanje računalne snage, veća zastupljenost pametnih telefona, manji troškovi senzora te za prikupljanje i pohrane podataka zbog cloud rješenja. Takva povezana budućnost donosi mnogo vrijednosti i mogućnosti za ljude.

Također, IoT postaje sve više specifičan za industriju te se proizvođači usredotočuju na projektiranje rješenja za određene industrije i segmente industrije. Sve je veća potražnja za specifičnim slučajevima uporabe koji pomažu u rješavanju izazova specifičnih za industriju. Na primjer, IoT rješenja za daljinsko praćenje pacijenata s ciljem smanjenja troškova i poboljšanja kvalitete njege pacijenata.

Nova područja također se pojavljuju između međusobno povezanih tehnologija i različitih područja kao što je medicina, industrija, pametni gradovi, pametne zgrade, pametna poljoprivreda, itd. IoT će se nastaviti spajati s drugim tehnologijama jer pruža daleko više mogućnosti u kombinaciji s njima, kao što je primjerice *blockchain*, umjetna inteligencija, strojno učenje, Big data i cloud.

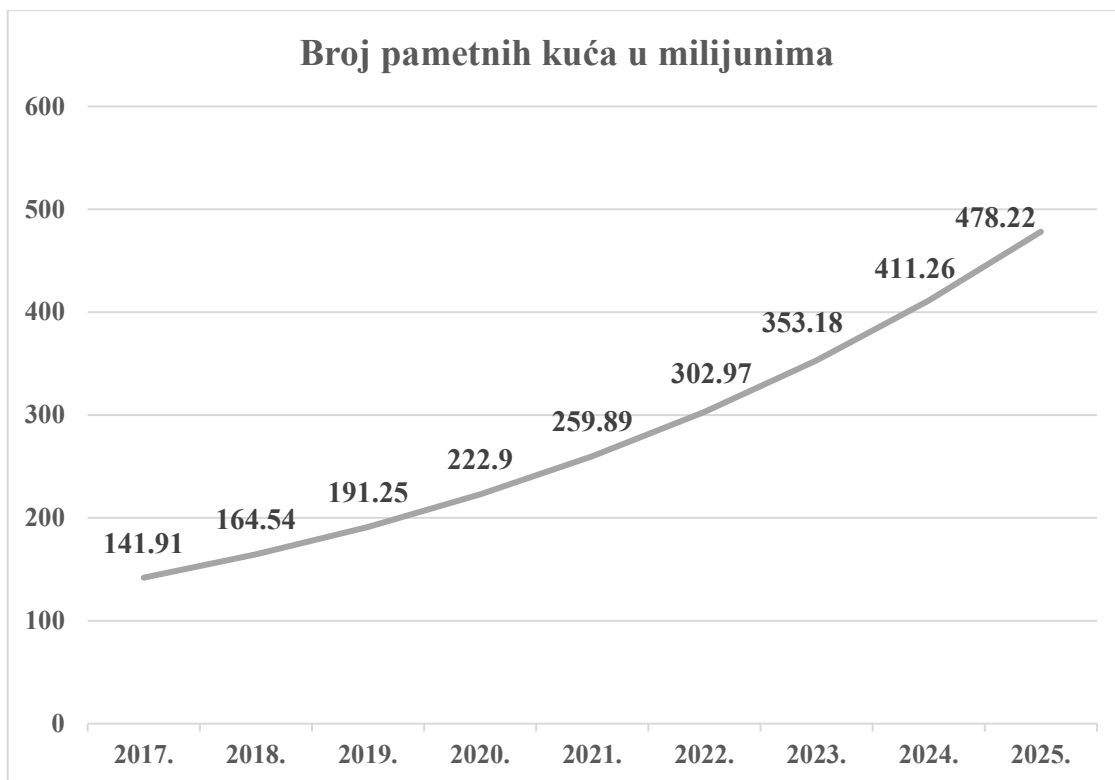
Budućnost IoT-a usko je povezana s umjetnom inteligencijom i strojnim učenjem. Primjeri aplikacija uključuju predviđanje održavanja međusobno povezanih uređaja, samooptimizaciju proizvodnih procesa i pametnih kućnih uređaja koji uče prema

korisnikovim preferencama. Predviđa se da uređaji neće samo izvještavati o informacijama, već će i donositi autonomne odluke i sami postajati pametniji primjenom tehnika strojnog učenja, [3]. Na grafikonu 1, nastavno na dosadašnje stanje broja povezanih uređaja, vidljivo je povećanje istih u naredne četiri godine, gdje broj IoT uređaja znatno premašuje ostale uređaje, što je još jedna potvrda kako različita područja idu u smjeru povezivanja ili prilagodbe na IoT.



Grafikon 1. Broj povezanih uređaja u narednim godinama izražen u milijardama, [14]

Paralelno s rastom povezanih uređaja, grafikon 2 prikazuje rast zastupljenosti pametnih kuća, koje su u fokusu ovoga rada, što dokazuje pozitivan trend automatizacije tradicionalnih kućanstava te ide u prilog svemu zaključenom do sada. ,

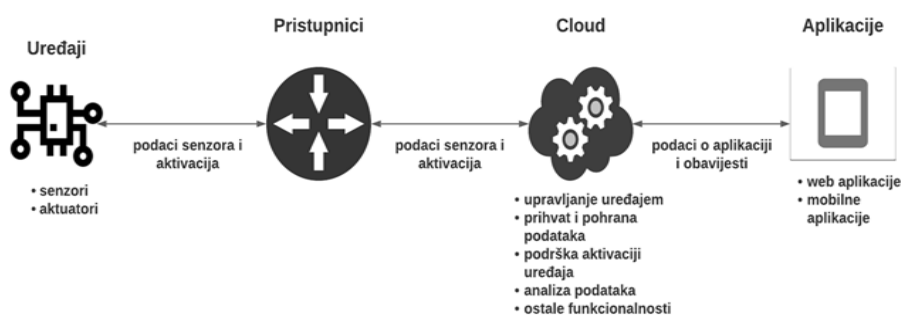


Grafikon 2. Broj pametnih kuća izražen u milijunima, [14]

3. Programska podrška za koncept IoT

Mobilno računalstvo, web aplikacije i softver kao usluga (eng. *Software as a Service* - SaaS) postaju sve više standardni, što znači da će svakodnevne stvari u okruženju postati povezanije i pogodnije programiranju. Učinak navedenog pretpostavlja se da će biti jednako bitan kao i revolucija mobilnih aplikacija što se smatra sličnim tehnološkim napretkom. Tražena iskustva programiranja se temelje na raznim Internet stvarima. Isključivo one vještine koje su najraširenije među većinom programera danas, poput poznavanja web razvoja ili razvoja aplikacija Android ili iOS uređaja, same neće biti dovoljne. Povrh toga, razvojni projekti IoT-a zahtijevaju znanje barem četiri različita područja razvoja softvera kao što su ugrađeni, cloud, web i mobilni softver. Brzi razvojni ciklusi koji su karakteristični za današnje softverske sustave temeljene na cloudu rezultiraju dodatnim izazovima i složenosti zadatka.

IoT omogućuje digitalne podatkovne proizvode i usluge, donoseći novu vrijednost i inteligenciju stvarima. To podrazumijeva preuzimanje prethodno nepovezanih uređaja, njihovo povezivanje s internetom i dodavanje pozadinske usluge te web i/ili mobilnih aplikacija za pregled, analizu i kontrolu zbog uvođenja nove vrijednosti i pogodnosti. S obzirom na povezanu prirodu pametnih stvari i potrebu za pozadinsku uslugu IoT sustavi su *end-to-end* (E2E) sustavi koji se sastoje od niza elemenata koji su gotovo identični u svim IoT sustavima, [16].



Slika 7. E2E IoT arhitektura, [16]

Elementi IoT sustava vidljivi su na slici 7 pri čemu su uređaji hardverski elementi koji prikupljaju podatke senzora i mogu pokrenuti aktivaciju. Pristupnici prikupljaju, predprocesiraju i prenose podatke senzora iz uređaja i omogućuju aktiviranje zahtjeva iz

clouda prema uređajima. Cloud ima niz važnih uloga, uključujući upravljanje uređajem, prikupljanje podataka, pohranu i pristup podacima, analitiku podataka u stvarnom vremenu i/ili izvan mreže te aktiviranje uređaja. Aplikacije mogu biti od jednostavnih ploča za vizualizaciju podataka temeljenih na webu pa sve do web i mobilnih aplikacija specifičnih za ovo područje. Nadalje, obično je potrebna neka vrsta administrativnog web korisničkog sučelja, [16].

Na prvi pogled, razvoj softvera za IoT sustave se ne razlikuje mnogo od bilo kojeg drugog oblika razvoja softvera. Kada programeri rade na svom prvom razvojnom projektu IoT-a, obično ciljaju jednostavan sustav koji se sastoji jednog uređaja, ploče (npr. Arduino) ili male, relativno homogene kombinacije takvih uređaja. Međutim, IoT sustavi u stvarnom svijetu obično su mnogo složeniji, sastoje se od mnoštva IoT uređaja i rješenja za više pristupnika, cloud i pozadinsku analitiku. Većina izazova u razvoju IoT-a proizlazi iz raspodijeljene i isprekidane prirode sustava, potencijalno nepouzdanosti i dugih kašnjenja. U kompleksnim sustavima, broj IoT uređaja također se može dinamički mijenjati. Potencijalno nepredvidiva, vrlo dinamična priroda E2E sustava predstavlja dodatni teret programerima. Nadalje, znatno brži ciklusi implementacije i razvojne metode karakteristične za današnje cloud zasnovane softverske sustave rezultiraju i dodatnim složenostima, posebno ako je tisuće zemljopisno raspoređenih uređaja potrebno istovremeno ažurirati, [16].

3.1. Programska podrška za uređaje koncepta IoT

Prvi navedeni element u E2E arhitekturi su uređaji. *Low-end* uređaji mogu biti bez operativnog sustava ili ih može pokretati operativni sustav koji radi u stvarnom vremenu. Većina današnjih IoT uređaja je relativno jednostavna. Primjerice, uređaji poput pametnog termostata, pametne brave ili senzora za kvalitetu zraka inače ne zahtijevaju složen softver. U svrhu implementacije jednostavnog sučelja detekcije i aktivacije, obični mikrokontroler sa osnovnim driverima za detekciju i aktivaciju je sasvim dovoljan. Za ponešto kompleksnije i sposobnije uređaje s većim setom senzora može biti potreban operativni sustav koji radi u stvarnom vremenu, kao što je primjerice RTOS. Standardni programski jezik za *low-end* sustave je C ili C++, iako se u nekim područjima može primijeniti i asemblerski jezik. Dostupnost cijenom veoma prihvatljivog hardvera usmjerava IoT prema uporabi sposobnijih i kompleksnijih uređaja. Kod jednostavnih IoT uređaja nema potrebe za programiranjem samih

uređaja od treće strane jer se sva ažuriranja softvera odvijaju ažuriranjem *firmwarea*. No, s obzirom na brzorastuće sposobnosti i mogućnosti hardvera, raste i izvedivost dinamičkog programiranja uređaja i kod najjeftinijih uređaja. Primjerice, Raspberry Pi ploče mogu podržavati operativni sustav kompatibilan Linuxu po vrlo niskoj cijeni. Često može izgledati jednostavnije i prihvatljivije kupiti opisani hardver nego složena hardverska rješenja jer zbog navedenog čak i jeftini uređaji mogu premašiti razinu korisnikove stvarne potrebe, [17].

Mnogo je različitih razina softvera IoT uređaja. Kao dodatak jednostavnim uređajima, postoje IoT razvojne ploče koje podržavaju specifične integrirane programske jezike ili virtualne strojeve. Na primjer, Espruino IoT razvojna ploča podržava JavaScript aplikacije, dok WiPy ploča podržava razvoj korištenjem Pythona. Sljedeću razinu uređaja predstavljaju uređaji poput prethodno spomenutog Raspberry Pi koji mogu pokrenuti operativni sustav (obično baziran na Linuxu) uz minimalne zahtjeve radne memorije, [17].

High-end uređaji sadrže softver koji se može usporediti s trenutnim softverom na mobilnim uređajima. To su primjerice nosivi uređaji kao što je watchOS ili Android Wear čija je platforma veoma slična navedenim mobilnim uređajima. Ovakvi sustavi omogućuju veoma bogat API (Application User Interface), ali daleko premašuje standardne minimalne hardverske zahtjeve. Primjerice, minimalna količina radne memorije za Android Wear je 512 MB, što je preko 10000 puta više od radne memorije potrebe jednom senzorskom uređaju. Softver uvelike ovisi o očekivanom korištenju istoga, štednji energije i potrebi za podržanim dinamičkim programiranjem ili daljnjim razvojem. Također, variraju i razvojne sposobnosti potrebne za određeni uređaj.

3.2. Programska podrška za pristupnike u konceptu IoT

Drugi element u E2E arhitekturi je pristupnik. On ima središnju ulogu u IoT sustavima. Primarno služi povezivanju IoT uređaja i clouda te prosljeđivanju zahtjeva aktivacije od clouda ka uređajima, omogućujući prijenos podataka koje su prikupili IoT uređaji na cloud. S obzirom da većina IoT uređaja podržavaju lokalnu povezanost temeljem tehnologija kao što su Bluetooth ili ZigBee, uređaji nisu u mogućnosti samostalno razmjenjivati informacije ili podatke s cloudom. Iz tog razloga postoji pristupnik kao nužno rješenje. Kao dodatak povezanosti i prijenosu podataka, pristupnici mogu obraditi podatke i pokretati analitičke

algoritme kako bi filtrirali i izabrali najrelevantnije podatke prije samog prijenosa. Mogu također generirati upozorenja kada vrijednosti podataka prekorače određene predefinirane raspone. S obzirom da pristupnici inače posjeduju veću računalnu moć od IoT uređaja, automatski postoji i potreba za većim računalnim sposobnostima kako bi se iznijeli izazovi E2E rješenja.

Pristupnici koji se danas koriste mogu se podijeliti u dvije kategorije ovisno o vrsti IoT sustava u uporabi. IoT softver orijentiran korisnicima potrošačima obično koriste pametne mobilne uređaje kao pristupnike. Primjerice, pametni satovi se često uparuju s korisničkim pametnim mobilnim uređajima, koristeći isti za prijenos podataka i ažuriranje uređaja. IoT profesionalni softver koji ima posebne zahtjeve koji zahtijevaju specijalizirana rješenja pristupnika predstavlja drugu kategoriju. Primjerice, u aplikacijama koje se koriste u industrijske svrhe, postoji potreba za uređajima koji su otporni na vodu, prašinu ili vibracije.

Softver neophodan za razvoj pristupnika varira od mobilnog razvoja sve do razvoja integriranih sustava. Zahtjevi računalne sposobnosti pristupnika uvelike ovise o tome je li se pristupnici koriste za jednostavno prikupljanje i prosljeđivanje podataka u cloud ili se od njih očekuju značajniji izvedbeni procesi kao što su kompleksna analitika i algoritmi, [16].

3.3. Programska podrška za cloud i analitiku koncepta IoT

Treći element u zajedničkoj E2E IoT arhitekturi prikazanoj na slici 7 je cloud. Razvoj clouda značajno je napredovao u posljednjem desetljeću. Cloud postaje sve zanimljivije područje krajem 1990-ih. Tada su programeri morali postaviti vlastite fizičke poslužitelje i upravljati vlastitim podatkovnim centrima. Osim *web* poslužitelja i softvera za baze podataka, gotovo sav razvoj softvera morao se raditi . Danas su gotovo sve potrebne implementacijske komponente dostupne besplatno kao otvorene komponente. Nadalje, dostupnost javnih usluga u cloudu, poput Amazon Web Services (AWS), IBM Cloud ili Microsoft Azure olakšao je postavljanje okruženja u cloudu bez potrebe za kupnjom ili posjedovanjem bilo kojeg fizičkog poslužiteljskog hardvera. Središnji elementi tipičnog *back-end* rješenja IoT clouda prikazani su na slici 8 koja se temelji na nekim od razvojnih projekata industrijskog IoT-a.



Slika 8. IoT cloud *back-end* arhitektura, [16]

Danas se gotovo sva komponentna područja prikazana na slici 8 mogu izgraditi pomoću tehnologija otvorenog koda. Na primjer, pri postavljanju sigurnosnog perimetra programeri obično koriste HAProxy ili NGINX. Za prikupljanje podataka popularno je rješenje Apache Kafka. Za analitiku podataka postoje različita rješenja ovisno o tome je li primarni fokus na analitici u stvarnom vremenu ili izvan njega. Za prvotno područje, programeri obično koriste Apache Storm, dok vanmrežnom analizom dominira Apache Hadoop. Za bilježenje i praćenje, popularna su rješenja poput Graphite i Icinga. S obzirom na dostupnost i zrelost komponenti otvorenog koda, uloga *back-end* programera danas bi se mogla više okarakterizirati kao sastav softvera ili upravljanje umjesto tradicionalnog razvoja softvera. U takvom razvoju, kod koji su napisali sami programeri čini samo mali dio, dok većina sustava dolazi iz otvorenog koda koji su napisale treće strane. Umjesto izgradnje IoT cloud rješenja od dostupnih *open source* ili komercijalnih komponenti, također je moguće unajmiti cijeli IoT *back-end* kao uslugu. Postoje popularne IoT cloud usluge poput Amazon AWS IoT, Microsoft Azure i Nokia IMPACT IoT platforme koja se može koristiti za povezivanje IoT uređaja uz redovitu naknadu. Postoje i opcije dobavljača IoT cloud usluga koji mogu postaviti IoT cloud za određene korisnike i upravljati tim cloudom u ime kupaca. Općenito, razvoj *back-enda* IoT-a postao je vrlo popularno područje posljednjih godina. Kao što je gore prikazano, okruženjem razvoja clouda dominiraju tehnologije otvorenog koda. Prema statistici, 91% IoT

programera koristi softver otvorenog koda barem jedan dio razvojnog procesa. Dostupnost tehnologija komponenti otvorenog koda i javnog clouda dovela je do širenja IoT clouda. Nedavna studija pokazala je da postoji više od 120 komercijalnih IoT cloud rješenja, [16].

3.4. Programska podrška za aplikacije koncepta IoT

Četvrti element u arhitekturi E2E IoT sustava su aplikacije. Pod aplikacijama se podrazumijevaju one koje se koriste za vizualizaciju podataka prikupljenih IoT uređajima, kao i za upravljanje i kontrolu uređaja. Ove se aplikacije mogu općenito podijeliti u tri kategorije: mobilne, web i računalne aplikacije. IoT aplikacije razvijene su i raspoređene u nekoliko domena kao što su transport i logistika, zdravstvo, maloprodaja i lanac opskrbe, industrija, okoliš, pametne kuće i sl. Unatoč njihovoj sveprisutnosti, razvoj IoT aplikacija i dalje nailazi na prepreke zbog toga što uključuje rješavanje nekoliko povezanih problema, kao što su nedostatak odgovarajuće identifikacije uloga različitih elemenata sustava, kao i nedostatak odgovarajućih okvira za rješavanje heterogenosti u IoT sustavima. Te poteškoće povećavaju vrijeme razvoja, resurse i odgađaju implementaciju IoT aplikacija, [18].

4. Podatkovni protokoli i komunikacijske tehnologije

Podatkovni protokoli koji služe za razmjenu informacija i podataka između poslužitelja i uređaja te između uređaja jedan su od najbitnijih dijelova IoT sustava. U ovom poglavlju opisat će se MQTT, XMPP, DDS i AMQP protokoli kako bi se dobio što bolji uvid u način komunikacije između navedenih elemenata. Također, opisat će se i najzastupljenije komunikacijske tehnologije kao što je NFC, RFID, Bluetooth, WiFi te ZigBee.

4.1. Protokoli za prijenos podataka

D2D (eng. *Device to Device*) predstavlja osnovni slučaj korištenja protokola u kojem uređaji komuniciraju međusobno. Nadalje, prikupljanje i slanje istih podataka na poslužitelju predstavlja slučaj korištenja D2S (eng. *Device to Server*), dok S2S (Server to Server) predstavlja daljnje dijeljenje podataka između poslužitelja te mogućnost vraćanja informacija uređajima, korisnicima ili softveru za analizu, [19].

Podatkovni protokoli u razmjeni informacija i podataka omogućuju točnost i pravovremenost. S obzirom da se u IoT-u koristi mnogo različitih protokola, veoma ih je bitno kategorizirati ovisno o namjeni i o adresiranju podataka:

- MQTT (eng. *Message Queue Telemetry Transport*) predstavlja protokol za prikupljanje podataka od uređaja te prijenos na poslužitelj (D2S).
- XMPP (eng. *Extensible Messaging and Presence Protocol*) je protokol pogodan za komunikaciju između korisnika i uređaja (specifični D2S jer su korisnici spojeni na poslužitelj).
- DDS (eng. *Data Distribution Service*) protokol je koji se koristi za brzu komunikaciju između uređaja (D2D)
- AMQP (eng. *Advanced Message Queuing Protocol*) protokol koji se odnosi na sustav čekanja koji služi za povezivanje poslužitelja (S2S), [19].

4.1.1. MQTT protokol

Načela dizajna ovog protokola usredotočena su na smanjenje propusnosti mreže i osiguravanje zahtjeva resursa uređaja osiguravajući pouzdanu isporuku. Pouzdan je za prijenos podataka putem niskopojasnih ili nepouzdatih mreža. Karakteristike poput lagane, otvorene, jednostavne i lake primjene čine MQTT najpogodnijim komunikacijskim protokolom za ograničena okruženja. Funkcionira putem TCP/IP-a ili preko drugih mrežnih protokola koji omogućavaju dvosmjerne veze bez gubitaka. MQTT pruža tri razine kvalitete usluge za dostavu poruka, [20].

Prva kvaliteta usluge je QoS 0 (eng. *Quality of Service*). Na toj razini kvalitete usluge poruke se isporučuju najviše jednom u skladu s radnim okruženjem. Mogućnost za gubitak poruke ostaje nepromijenjena. Primjer slučaja uporabe QoS 0 je slanje podataka tlaka, vlažnosti i temperature u stvarnom vremenu aplikaciji za daljinsko očitavanje gdje nije važno hoće li se veza s aplikacijom za čitanje podataka izgubiti na neko vrijeme.

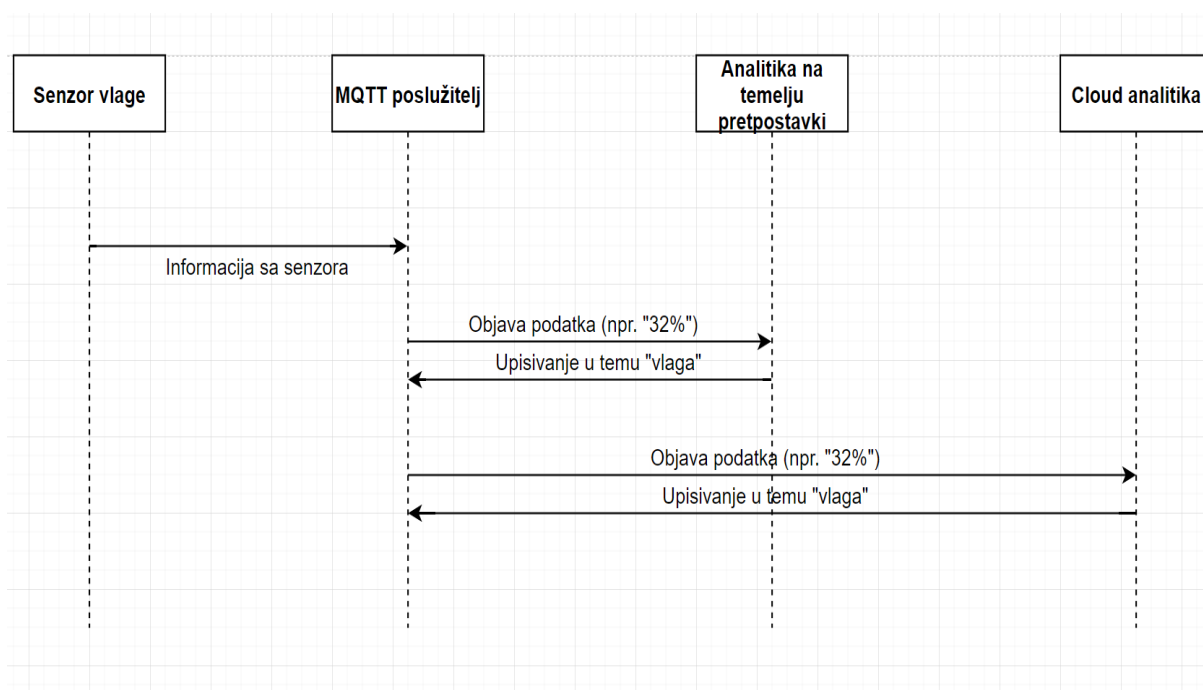
Druga i treća kvaliteta usluge su QoS 1 i QoS2. Na prvotnoj razini usluge poruke moraju biti isporučene barem jednom, a može doći do dvostrukosti. Što se tiče treće kvalitete usluge, u njoj je osigurano da se poruke isporučuju točno jednom te je karakterističan mali promet i razmjena između protokola je svedena na minimum kako bi se smanjio mrežni promet. Ova je usluga korisna za obavješćavanje zainteresiranih strana kada dođe do neobičnog prekida veze. Primjerice, ova razina se koristi kod sustavima naplate gdje redundantnost gubitka poruka može dovesti do nametanja netočnih troškova, [20].

MQTT ima tri sastavne komponente:

1. Izdavač (MQTT klijent)
2. Posrednik (MQTT poslužitelj)
3. Potrošač / pretplatnik (MQTT klijent)

MQTT klijent je program ili uređaj koji koristi MQTT protokol. Klijent je odgovoran za otvaranje mrežne veze s poslužiteljem, kreiranje poruka za upisivanje, upisivanje poruka aplikacija na poslužitelju, pretplatu na zahtjeve aplikacija koje želi primati, otkazivanje pretplate radi uklanjanja zahtjeva za poruke aplikacije i zatvaranje mrežne veze na

poslužitelju. Poruka aplikacije odnosi se na podatke koje prenosi MQTT protokol preko mreže za aplikaciju. Sve poruke aplikacije koje prenosi MQTT sadrže podatke o opterećenju, QoS-u te zbirku svojstava i naziv teme. MQTT poslužitelj je program ili uređaj temeljen na MQTT -u koji djeluje kao poštanski ured između izdavača i pretplatnika. MQTT posrednik odgovoran je za prihvaćanje mrežnih veza od klijenata, prihvaćanje poruka aplikacija koje su klijenti objavili, obradu zahtjeva od klijenata za pretplatu i odjavu, slanje aplikacijskih poruka klijentima prema svojim pretplatama i zatvaranje mrežne veze od strane klijenta.



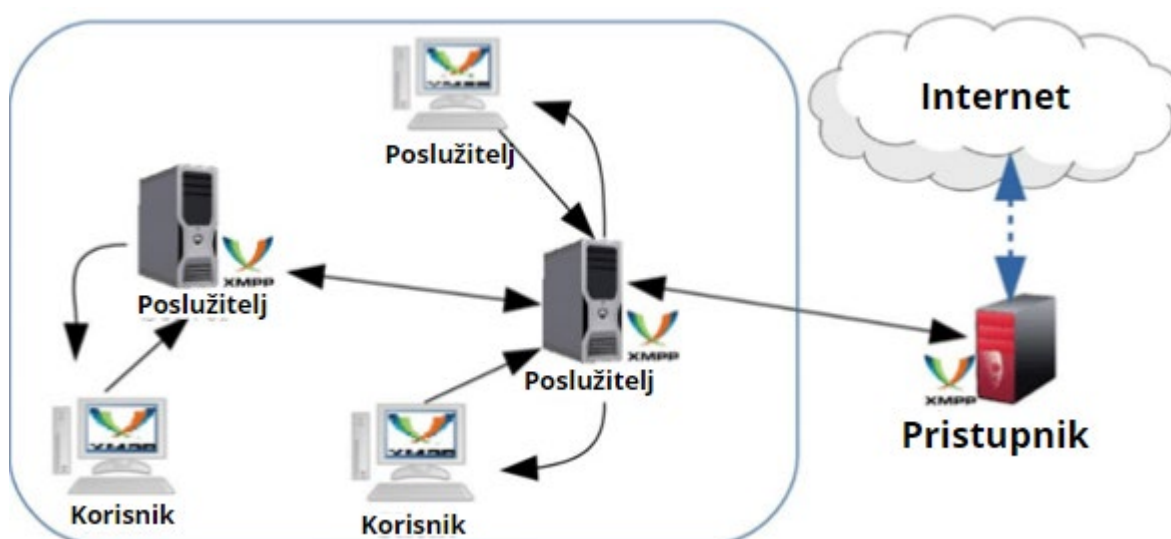
Slika 9. Dijagram slijeda MQTT u arhitekturi IoT, [21]

MQTT je također dvosmjerni komunikacijski protokol, što pomaže u razmjeni podataka, upravljanju i kontroli uređaja, a njegova funkcionalnost unutar IoT arhitekture u sklopu dijagrama slijeda prikazana je na slici 9, [20].

4.1.2. XMPP protokol

XMPP je protokol aplikacijskog sloja za razmjenu podataka u stvarnom vremenu i usluge zahtjeva i odgovora između više entiteta na mreži. XMPP se u početku uglavnom koristio kao komunikacijski protokol koji je prvenstveno dizajniran za usluge razmjene trenutačnih poruka za platforme kao što su Google Hangouts i WhatsApp Messenger. Tijekom godina ovaj je protokol primijenjen u uslugama poput VoIP-a. U posljednje vrijeme XMPP je postao široko

primijenjen u IoT aplikacijama te se obično provodi pomoću arhitekture klijent-poslužitelj gdje klijenti i poslužitelji komuniciraju putem TCP veze. Budući da je otvorenog koda i široko se primjenjuje, XMPP se smatra pouzdanim i sigurnim protokolom za upotrebu u IoT aplikacijama, osobito u scenarijima u kojima je uređajima potrebna dvosmjerna komunikacija sa poslužiteljima ili gdje dva udaljeno povezana uređaja moraju međusobno razmjenjivati poruke. XMPP protokol ocrta format za razmjenu podataka između dva ili više komunikacijskih uređaja, što u slučaju IoT ekosustava može biti između senzora i aktuatora (D2D) ili između senzora, aktuatora, poslužitelja i clouda (D2S/C), [22].



Slika 10. XMPP protokol, [22]

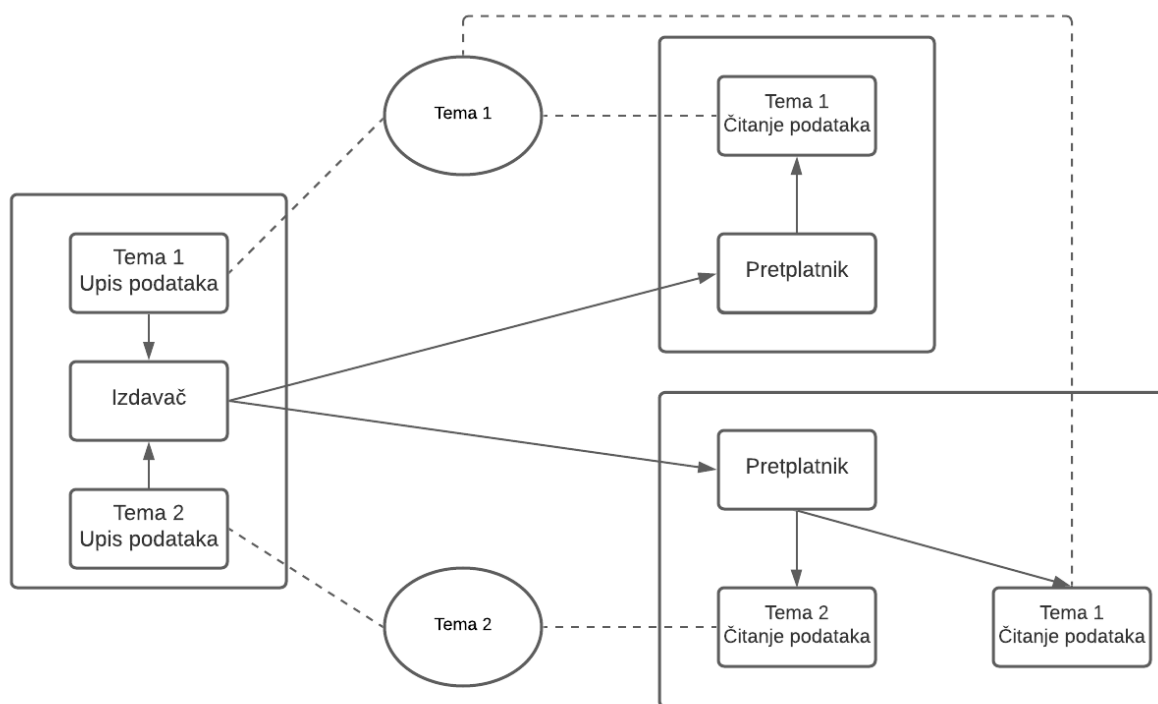
Sva komunikacija se odvija putem odgovarajućeg poslužitelja koji zatim prosljeđuje poruku klijentu koji se nalazi pod drugim poslužiteljem, kako je prikazano na slici 10. XMPP koristi jedinstveni identifikator koji je dodijeljen svakom uređaju za identifikaciju. Dio naziva domene je obvezni zahtjev i sadrži razlučivi DNS naziv entiteta koji bi mogao biti poslužitelj, komponenta ili dodatak.

4.1.3. DDS protokol

DDS (eng. *Data-Distribution Service*) predstavlja međunarodni standard za povezivanje koji integrira komponente sustava, pružajući prijenos podataka s malim kašnjenjem, velikom pouzdanosti i skalabilnom arhitekturom, što ga čini idealnim za industrijske primjene od pametnog transporta, pametnih tvornica, pametnih gradova, itd. Usmjeren je isključivo na podatke te njima upravlja, kontrolira i dijeli ih. Korisnici mogu pouzdano i sigurno iskoristiti veće količine podataka koje generira uređaj i obrađuje podatke u stvarnom vremenu, a zatim

djeluju na događaje onoliko brzo koliko se oni pojave. Kao rezultat, DDS omogućuje pametnije odluke, nove usluge, dodatne izvore prihoda i smanjene troškove. Bogat je značajkama koji transparentno rješavaju velik dio složenosti podatkovnog povezivanja industrijskog IoT sustava, [23].

Standard DDS pojednostavljuje razvoj, implementaciju i upravljanje IoT aplikacijama, ubrzavajući vrijeme do izlaska na tržište. To omogućuje lakoću integracije (DDS pristup usmjeren na podatke omogućuje definiranje zajedničkih i proširivih modela podataka za besprijekornu interoperabilnost informacijskih i operativnih tehnologija), učinkovitost izvedbe (implementacije mogu postići vrlo male latencije od točke do točke i protok od nekoliko milijuna poruka u sekundi), skalabilnost (arhitektura je skalabilna od malih uređaja do clouda, povezujući tisuće uređaja i sustava dostavljajući podatke iznimno velikom brzinom) i naprednu sigurnost (sigurnosna specifikacija definira opsežan sigurnosni model i dodatak za usluge arhitekture za usklađene implementacije DDS -a). Bogat skup QoS politika omogućuje DDS-u kontrolu svih aspekata distribucije podataka, kao što su pravovremenost, određivanje prioriteta prometa, pouzdanost i korištenje resursa. Također, implementacije podržavaju više programskih jezika, operativnih sustava i platformi za posluživanje, od poslužitelja u cloudu do mobilnih uređaja, mikrokontrolera, itd.



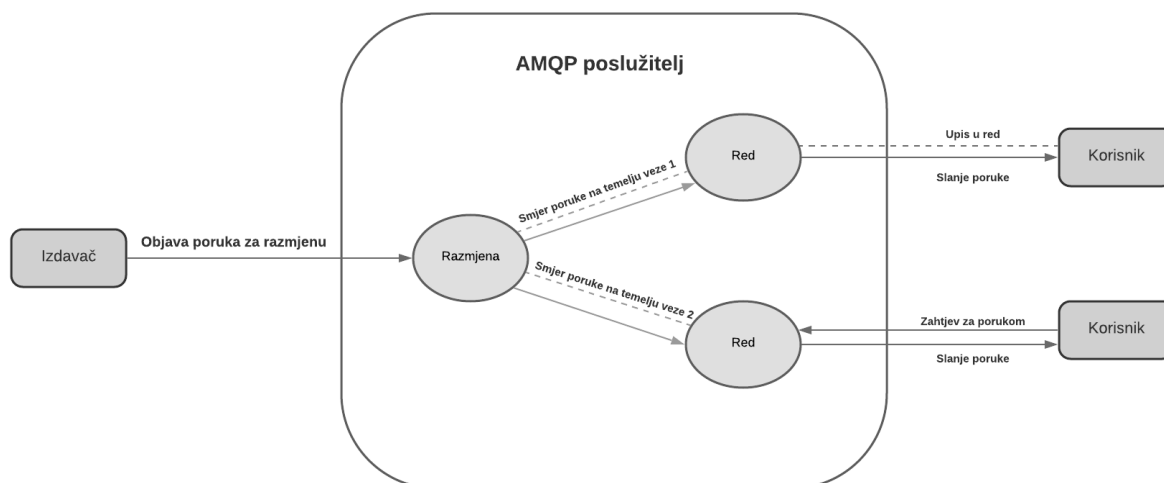
Slika 11. Arhitektura DDS protokola, [24]

DDS komunikacija je *peer-to-peer*. Uklanjanje posrednika za poruke i poslužitelja pojednostavljuje implementaciju, minimizira kašnjenje, maksimizira skalabilnost, povećava pouzdanost i smanjuje troškove i složenost. Idealan je za IoT aplikacije koje zahtijevaju dugotrajnu i pouzdanu arhitekturu visokih performansi. Arhitektura DDS protokola prikazana je na slici 11, [23].

4.1.4. AMQP protokol

AMQP je M2M protokol, za razmjenu poruka osmišljen za pouzdanost, sigurnost i interoperabilnost. Nudi širok raspon značajki povezanih s razmjenom poruka, poput pouzdanog čekanja u redu, temeljenog na temama upisivanja i pretplate na poruke, fleksibilnog usmjeravanje i transakcije, [25].

Kao što je prikazano na slici 12, komunikacijski sustav AMQP zahtijeva da izdavač ili korisnik kreira "razmjenu" s datim imenom, a zatim emitira taj naziv. Izdavači i korisnici koriste naziv ove razmjene kako bi otkrili jedni druge. Nakon toga korisnik stvara "red čekanja" i istovremeno ga priključuje na razmjenu. Poruke primljene razmjenom moraju se upariti s redom putem procesa koji se naziva "vezivanje".



Slika 12. Arhitektura AMQP protokola, [25]

AMQP razmjenjuje poruke na različite načine kao što je izravno, u obliku odjavljivanja, prema temi ili na temelju zaglavlja. AMQP je binarni protokol i obično zahtijeva fiksno zaglavlje s malim opterećenjem poruka do maksimalne veličine ovisno o poslužitelju ili

tehnologiji programiranja. AMQP koristi TCP kao zadani transportni protokol, a TLS ili SSL za sigurnost. Stoga je komunikacija između korisnika i poslužitelja orijentirana na povezivanje. Pouzdanost je jedna od temeljnih značajki AMQP -a, [25].

4.2. Komunikacijske tehnologije u primjeni

Glavna svrha IoT-a je kvalitetnije i brže pružanje usluga korisnicima u raznim okruženjima, a to je moguće samo kada je osigurana besprijekorna povezanost. Neke usluge koje zahtijevaju visoku preciznost posebno zahtijevaju visoku kvalitetu komunikacijskih tehnologija koje su prikazane na tablici 2. Primjerice, u slučaju pametnih kuća, kašnjenje u mreži može izazvati ozbiljne probleme. Zbog toga su određeni ciljevi za komunikacijske tehnologije poput vrlo visoke učinkovitosti spektra, prijenosa podataka visokim brzinama, niskom potrošnjom energije i visoke stabilnosti veze, [26].

Tablica 2. Karakteristike komunikacijskih tehnologija u IoT-u, [26]

	NFC	RFID	Bluetooth	Wi-Fi	ZigBee	LoraWAN
Mreža	PAN	PAN	PAN	LAN	LAN	LPWAN
Topologija	P2P	P2P	Zvezdasta	Zvezdasta	Zvezdasta, Razgranata	Zvezdasta
Snaga	Vrlo niska	Vrlo niska	Niska	Niska- Visoka	Vrlo niska	Niska
Brzina	400 Kbps	400 Kbps	700 Kbps	11-100 Mbps	250 Kbps	do 27 Kbps
Domet	< 10cm	< 3m	< 30m	4-20 m	10-300 m	< 10-15 km
Aplikacija	Pristup, plaćanje, dijeljenje	Praćenje predmeta	Razmjena podataka	Internet, multimedija	Senzorske mreže, automatizacija	Nadzor, upravljanje
Troškovi	Niski	Niski	Niski	Srednji	Srednji	Niski

Glavni zadatak komunikacijskih tehnologija je omogućavanje povezanosti između raznih pametnih uređaja, a među najbitnijima su: ZigBee, LoraWAN, Wi-Fi, Bluetooth, RFID i NFC. Karakteristike navedenih prikazane su u tablici 2 kao svojevrsna usporedba istih.

4.2.1. NFC

NFC (eng. *Near-field Communication*) označava beskontaktni prijenos podataka koji koristi tehnologiju radiofrekvencijske identifikacije, standardizirane frekvencije na 13,56 MHz te koji omogućuje prijenos u rasponu od pet do deset centimetara. Ova tehnologija koristi mobilne terminalne uređaje za razmjenu podataka. U osnovi, NFC se može podijeliti na tri različite vrste:

1. Način emulacije kartice – primjerice, pametni telefon preuzima funkciju beskontaktno kartice. To omogućuje otvaranje vrata kompatibilnih sa pametnim telefonima u hotelu ili pristup tvrtki, uz bilježenje odgovarajućeg vremena.
2. Način čitanja/pisanja - pomoću ovog načina rada pametni telefon čita sadržaj NFC oznake. Primjerice, to se može koristiti za pametne plakate. Koristeći aplikaciju, prislanjajući pametni telefon za oznaku koji je integriran u plakat, otvara se web stranica i pruža mogućnosti ovisno o prirodi sadržaja.
3. *Peer-to-peer* način rada - u ovom načinu rada odvija se komunikacija između dva mobilna uređaja. To podrazumijeva da se podaci, kontakti i slike mogu prenositi s jednog uređaja na drugi, [27].

Pasivne NFC oznake mogu se koristiti za označavanje gotovo svih objekata pri čemu ti objekti postaju „inteligentni“ i dobivaju pristup internetu. NFC sučelje već je integrirano u gotovo sve pametne telefone, što znači da je ova tehnologija standardizirana u cijelom svijetu i nudi širok raspon primjene. Svaka NFC oznaka ima jedinstveni identifikacijski broj u svijetu te je tako svaki proizvod jedinstven. Podaci na njoj se mogu nadopuniti, pročitati i promijeniti u bilo kojem trenutku.

4.2.2. Bluetooth

Ova tehnologija utemeljena je na IEEE 802.15.1 standardu. Predstavlja tehnologiju bežične komunikacije niske snage i niske cijene. Prikkladna je za prijenos podataka između mobilnih uređaja preko kratkog dometa (8-10 metara). Djeluje u rasponu od 2,4 GHz. Podatkovna stopa u različitim inačicama Bluetooth-a je u rasponu od 1 MB/s do 24 MB/s.

Bitna verzija je 4.2. koja je ujedno i uvod ove tehnologije u IoT sustav. Najbitnija stavka je Internet Protocol Support Profile verzija 6 koja je omogućila povezivanje uređaja u pametnim kućama Bluetoothom. Novijom verzijom 5, brzina transmisije se udvostručila i proširio se raspon djelovanja. Ova tehnologije se u sustavu pametne kuće najčešće pronalazi u mikroupravljačima koji kontroliraju rasvjetu, prekidače i utičnice, [28].

4.2.3. Wi-Fi

IEEE 802.16 predstavlja skup lokalnih bežičnih komunikacijskih standarda lokalnih bežičnih mreža. Na primjer, 802.11a djeluje u 5GHz rasponu. 802.11b i 802.11g djeluju u rasponu od 2.4 GHz, 802.11n djeluje u rasponima od 2.4/5 GHz, 802.11ac djeluje u rasponu od 5 GHz i 802.11ad djeluje u rasponu od 60 GHz. Wi-Fi pruža komunikacijski raspon od 20 metara (u unutrašnjosti) do 100 metara (u vanjskim prostorima), ovisno o optičkoj vidljivosti. Našao je primjenu u gotovo pa svim modernim uređajima današnjice. Uređaji kompatibilni za korištenje spajaju se na internet pomoću WLAN-a i bežičnih pristupnih točaka. Dvije najbitnije komponente su adapter i usmjernik (eng. *router*). Pomoću prvog se obavlja spajanje na mrežu, a pomoću drugog se dobiva izlaz na internet. Najvažniji protokoli su WEP, WPA i WPA2, [28].

4.2.4. RFID

Izraz IoT je bio prvenstveno predložen kao nešto što upućuje prema jedinstveno identificirajućim interoperabilnim objektima povezanim sa tehnologijom RFID (eng. *Radio-Frequency Identification*).

Prvotna svrha ove vrste industrijskog standarda većinom je ta da nastoji postići dobar dizajn kako bi se ostvario napredak u vidljivosti objekata, pogotovo kod objekata poznate lokacije i stanja. RFID još je uvijek glavna pokretačka snaga za IoT. Zbog niske cijene i male veličine, RFID dominira tržištem od svog nastanka. Za razliku od NFC tehnologije, koja je podskup RFID tehnologije, RFID se može koristiti na bilo kojoj frekvenciji i sadrži još drugih specifikacija. Također, bitna razlika je u dometu, gdje RFID radi i na većim udaljenostima, [28].

4.2.5. LoRaWAN

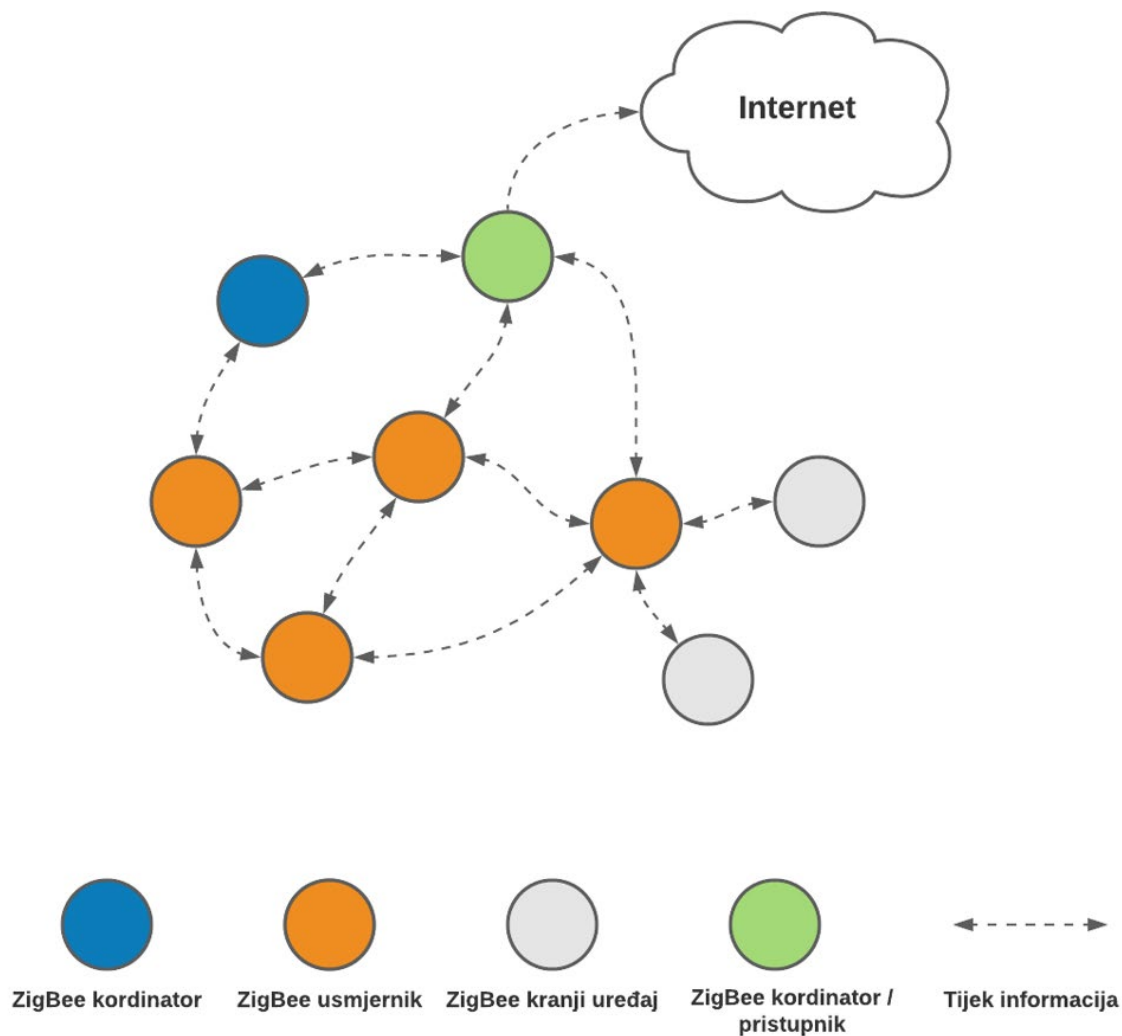
LoRaWAN je mrežni protokol male snage i širokog područja izgrađen na temelju tehnike radio-modulacije LoRa. Bežično povezuje uređaje s internetom i upravlja komunikacijom između uređaja s krajnjim čvorom i mrežnim pristupnikom. Upotreba LoRaWAN-a u industrijskim prostorima i pametnim gradovima i kućama raste jer je pristupačan, dvosmjerni komunikacijski protokol dugog dometa s vrlo niskom potrošnjom energije gdje uređaji mogu raditi deset godina na bateriji.

Krajnji uređaj može se povezati s mrežom pomoću LoRaWAN-a na dva načina:

- Aktivacijom bežičnim putem gdje uređaj mora uspostaviti mrežni ključ i ključ aplikacijske sesije za povezivanje s mrežom.
- Aktivacijom personalizacijom gdje je uređaj kodiran ključevima potrebnim za komunikaciju s mrežom, što omogućuje manje sigurnu, ali lakšu vezu, [29].

4.2.6. ZigBee

Jedan od korištenijih i zastupljenih standarda u automatizaciji kućanstava. Veoma je bitan jer, unatoč zatvorenosti glede pružanja podataka i pristupa, pruža standard za razvijanje novih sustava. Osnova ZigBee-a je radio standard IEEE 802.15.4. koji troši vrlo male količine energije te je prikladan standard za mnogo IoT aplikacija, iako nije baš najpovoljnije rješenje za veći broj uređaja ili za pokrivanje većih područja.



Slika 13. Topologija Zigbee mreže, [30]

ZigBee sustavno povezuje kućnu automatizaciju sa sustavom kontrole, rasvjete, brige o zdravlju i pametne kupovine. Na slici 13 prikazana je topologija mreže koja je kombinacija prstenaste strukture i PAN (eng. *Personal Area Network*) komunikacije. Unutar mreže postoje koordinatori koji upravljaju oblikom i zaštitom te su spona PAN-ovima. Uloga rutera je usmjeravanje podataka do terminalnih uređaja. Ovisno o postavkama, putem pristupnika može se omogućiti povezanost s internetom. Postoje još ZigBEE IP (osnova na IPv6 protokolu) te ZigBEE rf4ce specifikacije standarda, [30].

5. Planiranje IoT mreže

Planiranje predstavlja proces koji obuhvaća topološko projektiranje, sintezu mreže i realizaciju mreže, a ima za cilj osigurati da mreža ili usluga zadovolji potrebe korisnika i pružatelja usluge. Planirana mreža je učinkovita. Mrežno planiranje podrazumijeva izbjegavanje nepredvidivosti sustava koji se implementiraju bez temeljitog planiranja. Za planiranje mreže potrebno je obuhvatiti više područja. Primjerice, prepoznavanje aplikacija koje korisnici planiraju koristiti. Za umrežavanje mogu biti potrebna različita okruženja, poput upravljanja resursima, razmjene trenutnih poruka, e-pošte i drugih. Važno je pretpostaviti korisnikove buduće aktivnosti, korištenje aplikacija i slično jer se to koristi za procjenu softverskih, hardverskih i prometnih zahtjeva.

Prometni zahtjevi podrazumijevaju izračunavanje koje uključuje nekoliko čimbenika. Ono što treba uzeti u obzir je identifikacija i dokumentiranje glavnih izvora prometa, kategorizacija prometa kao lokalnog, distribuiranog, klijent/poslužitelj ili poslužitelj/poslužitelj prometa, procjenu zahtjeva propusnosti i kvalitetu usluge (QoS) za svaku aplikaciju te zahtjeve pouzdanosti i skalabilnosti. Skalabilnost je veoma bitan čimbenik iz razloga što se treba, pogotovo u mreži kao što je IoT, osigurati dodavanje i slično, [31].

. Prilikom planiranja mreže potrebno je razmotriti dostupnost mreže. To predstavlja vrijeme koje je mreža dostupna korisnicima u određenom vremenskom razdoblju. Sigurnost i pristupačnost također su među bitnijim čimbenicima planiranja mreže. faze Potrebno je izraditi sigurnosni plan koji zadovoljava tražene sigurnosne specifikacije. Bilo bi poželjno izraditi popis mrežnih usluga koje će se pružati, tko upravlja sigurnošću ovih usluga, kako se korisnika obučava o sigurnosnim politikama i procedurama, planu oporavka u slučaju da dođe do povrede sigurnosti i slično.

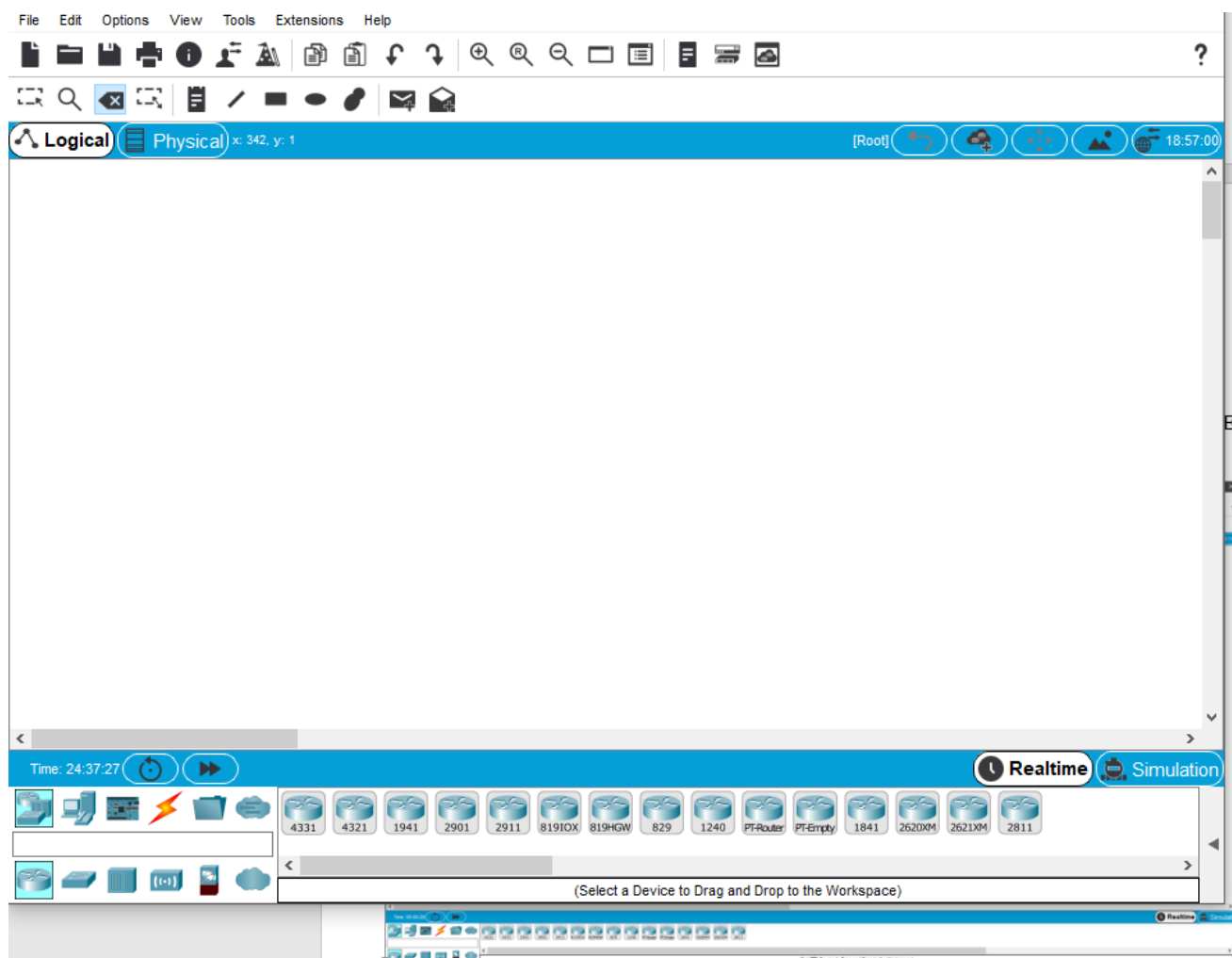
Također, potrebno je razmotriti i troškove izgradnje ovakve vrste mreže pri čemu se nastoji minimizirati troškove opreme. To minimizira troškove prijenosnih sustava, priključaka i troškove rada, [31]. U narednim poglavljima će se prvo opisati alat Cisco Packet Tracer u kojemu će se kasnije dizajnirati IoT mreža pomoću raznih funkcionalnosti i opcija kao što su različiti krajnji uređaji, pristupnici, usmjernici, mikrokontroleri i ostali.

5.1. Pregled Cisco Packet Tracer programske podrške

IoT mrežu moguće je kreirati unutar alata Cisco Packet Tracer koji u novijim verzijama podržava izradu i simulaciju iste. IoT nudi brojne mogućnosti upravljanja, nadzora i konfiguracije uređaja te njihovog međusobnog komuniciranja i djelovanja. Cisco Packet Tracer je alat za više platformi koji omogućuje mogućnost umrežavanja i simulacije IoT mreže bez posjedovanja hardvera ili mreže. Alat zapravo nudi opsežan skup hardvera i prijenosnih sustava koji omogućuju postavljanje od osnovne do vrlo složene mreže. Također objašnjava kako riješiti probleme s mrežom jer alat uključuje i realne značajke za ispravljanje pogrešaka. Od verzije 7.0 Cisco je također uveo IoT funkcionalnosti u alat, omogućujući vježbanje postavljanja IoT uređaja i IoT automatizacije. Također, postoji mogućnost za simulacije niže razine IoT-a korištenjem SBC (eng. *Single Board Computer*) i senzora, [32].

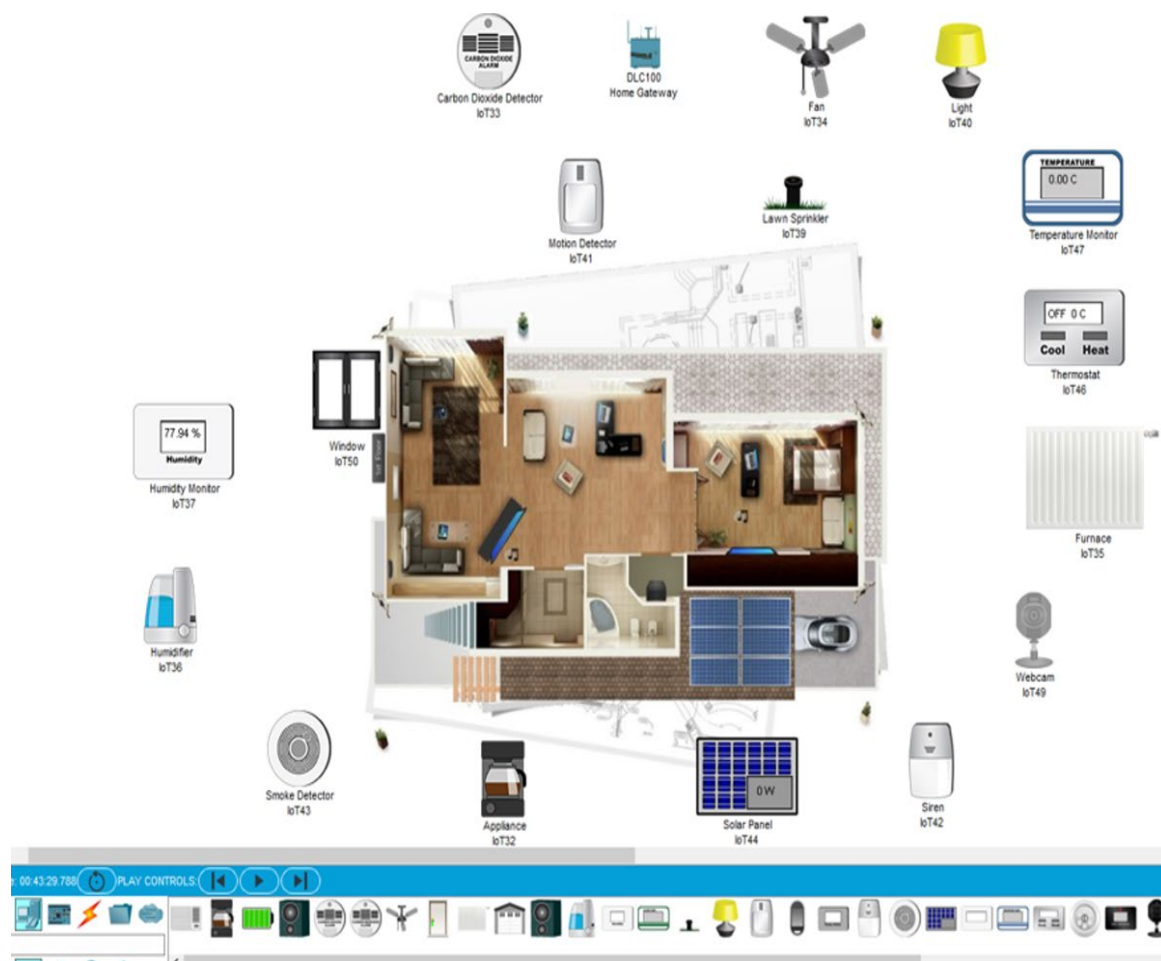
Glavna razlika koju treba uzeti u obzir pri konfiguraciji uređaja su moguća hardverska ograničenja koja dolaze s uređajima, u smislu broja dostupnih portova, mogućnosti promjene mrežnih sučelja, broj utora za proširenje itd. Opsežan popis sklopki, poslužitelja, računala i prijenosnog računala također je dostupan u alatu.

Grafičko sučelje, prikazano na slici 14, nudi brojne mogućnosti. Uz logički, postoji i fizički pregled postavljene mreže. Na dnu sučelja moguće je dodati brojne uređaje poput mrežnih, IoT uređaja unutar pametne kuće, pametnog grada, itd. Također, omogućen je izbor žičnog spajanja kabelima, kao i bežičnim tehnologijama kao što su Wi-Fi i Bluetooth. Mrežu je moguće promatrati u stvarnom vremenu i u simulacijskom načinu rada gdje je vidljiv i prometni tok uz naglašene protokole koji se koriste u komunikaciji.



Slika 14. Grafičko sučelje alata Cisco Packet Tracer

Na slici 15 prikazani su, zajedno s pozadinom preglednog plana kuće, mogući elementi pametne kuće u okviru alata kao što su uređaj za vlažnost zraka, senzor za mjerenje istoga, automatizirani prozor, detektor dima, pametni aparat za tople napitke, solarni panel, senzor pokreta, web kamera i ostali.



Slika 15. Mogućnosti dodavanja elemenata pametne kuće u okviru alata

Svaki element pametne kuće zahtijeva pojedinačnu konfiguraciju. Alat omogućuje fizički pregled uređaja dajući općenitu skicu funkcionalnosti rada, kao i opis značajki. Unutar istih je dat pregled funkcionalnosti, stanja, načina korištenja, povezivanja i kontroliranja samim uređajem.

Unutar konfiguracije prikazane na slici 16, moguće je odrediti pristup mreži preko pristupnika, izmijeniti postavke spajanja na poslužitelj, postaviti dodatne korake autorizacije ukoliko je potrebno te upravljati načinom spajanja uređaja. Uređaj je spojen na pristupnik žično ili bežično. Na primjeru sa slike 17 spajanje je izvedeno žično. Također, moguće je postaviti mogućnost ugrađenosti Bluetootha na uređajima. Na slici 18 prikazana je kartica naprednih mogućnosti gdje se određuje mrežni adapter, ovisno o vrsti povezanosti. Uređaj iz primjera postavljen je na bežični način povezivanja, koristi se kao pametni uređaj i u kartici programiranje moguće je napisati i skriptu programskog jezika koja će automatski odrediti ponašanje uređaja ovisno o scenariju koji se postavi.

Specifications Physical **Config** Attributes

GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
FastEthernet0

Display Name Svjetlo
Serial Number PTT08102G1Z-

Gateway/DNS IPv4
☐ DHCP
☒ Static
Gateway
DNS Server

Gateway/DNS IPv6
☐ DHCP
☐ Auto Config
☒ Static
IPv6 Gateway
IPv6 DNS Server

IoT Server
☐ None
☒ Home Gateway
☐ Remote Server
Server Address
User Name
Password

Slika 16. Konfiguracija uređaja

Specifications **IO Config** Physical Config Thing Editor Programming Attributes

Network Adapter	PT-IOT-NM-1W
Network Adapter 2	None
Digital Slots	1
Analog Slots	0
USB Ports	0
Bluetooth	☐ Built-in
Desktop	☐ Show
Usage	☒ Smart Device ☐ Component

Slika 17. Napredne mogućnosti konfiguracije uređaja

Na slici 18 prikazana je konfiguracija uređaja prilikom spajanja na bežičnu mrežu unutar pametne kuće gdje se uređaj postavlja automatski u smislu da se prepiše naziv SSID-a pristupnika (u ovom slučaju SSID1). Kao što je vidljivo, moguća je dodatna autentifikacija, ali je u ovom slučaju isključena. Konfiguracija IP-a je automatska pomoću DHCP protokola za dodjeljivanje IP adresa. Svaki uređaj unutar mreže ima svoju MAC adresu, također prikazanu u konfiguracijskoj kartici.

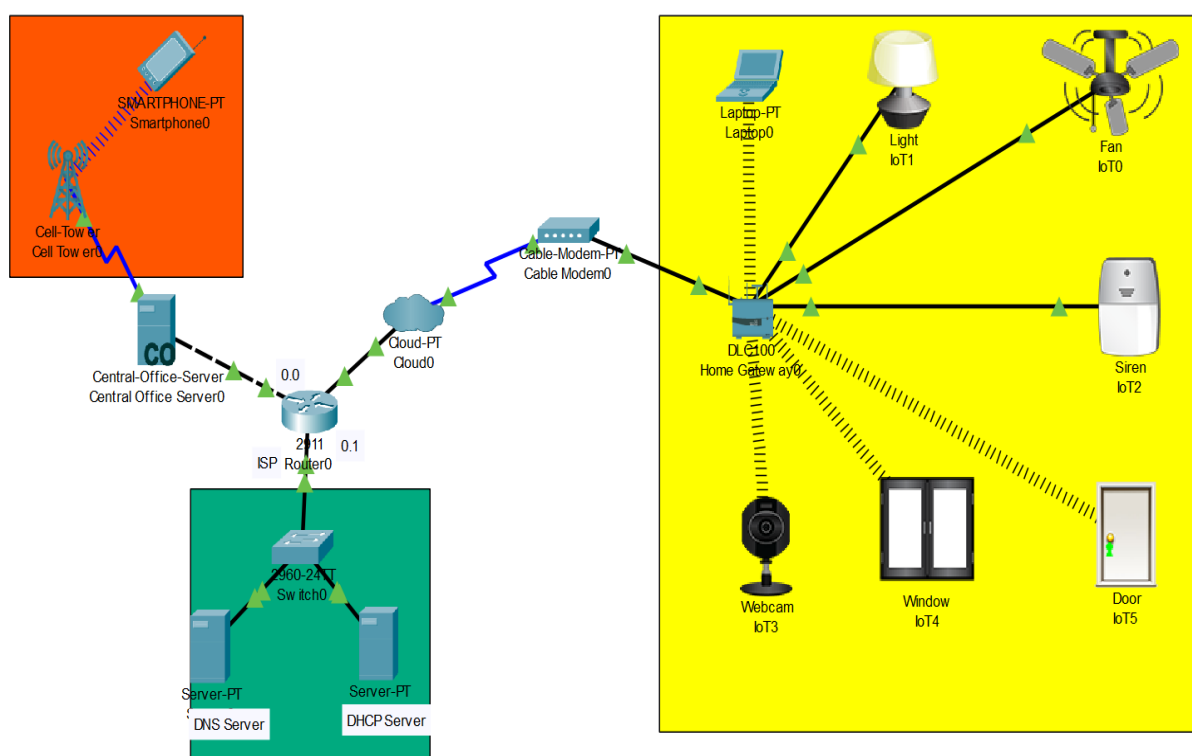
The image shows a configuration window for a network interface. On the left, a sidebar contains a tree view with 'GLOBAL' (containing 'Settings', 'Algorithm Settings', 'Files') and 'INTERFACE' (containing 'Wireless0'). The main panel is titled 'Wireless0' and contains several sections: 'Port Status' (empty), 'Bandwidth' (300 Mbps), 'MAC Address' (0002.16BD.C01E), and 'SSID' (SSID1). Below these is the 'Authentication' section with radio buttons for 'Disabled' (selected), 'WEP', 'WPA-PSK', 'WPA', and '802.1X'. To the right of these are fields for 'WEP Key', 'PSK Pass Phrase', 'User ID', 'Password', 'User Name', and another 'Password'. The 'Encryption Type' is set to 'Disabled'. The 'IP Configuration' section has radio buttons for 'DHCP' (selected) and 'Static', followed by fields for 'IP Address' and 'Subnet Mask'. At the bottom is an expandable 'IPv6 Configuration' section. At the very bottom of the window are a 'Top' button and an 'Advanced' button.

Slika 18. Konfiguracija povezivanja s bežičnom mrežom

5.2. Kreiranje IoT mreže unutar pametne kuće

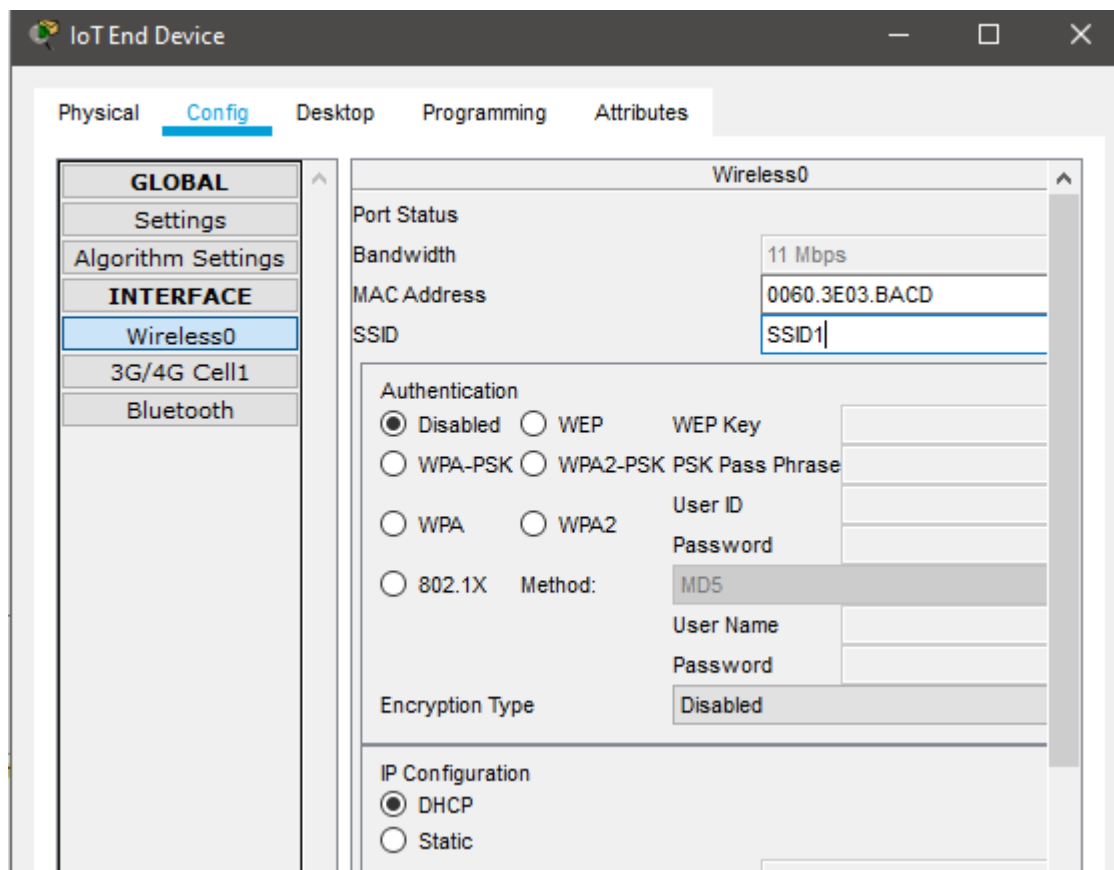
S obzirom da se obrađuje tematika IoT mreže unutar pametne kuće, većina rada će se oslanjati na arhitekturu mreže od pristupnika prema uređajima. No, kako bi se dobio bolji

uvid u stvarno korištenje sustava pametnih kuća iz korisničke perspektive, na slici 21 prikazan je pristup IoT mreži od korisničkog uređaja do krajnjih uređaja IoT mreže unutar pametne kuće. Na slici 19 također su prikazani su dijelovi mreže od korisničkog pametnog telefona koji se spaja na mrežu pružatelja mobilnih usluga preko kojeg je omogućen pristup cloudu, modemu te u konačnici i pristupniku unutar korisnikove pametne kuće gdje su prisutni uređaji koje može kontrolirati najčešće putem specijalizirane aplikacije. To korisniku otvara brojne mogućnosti upravljanja udaljenim putem.

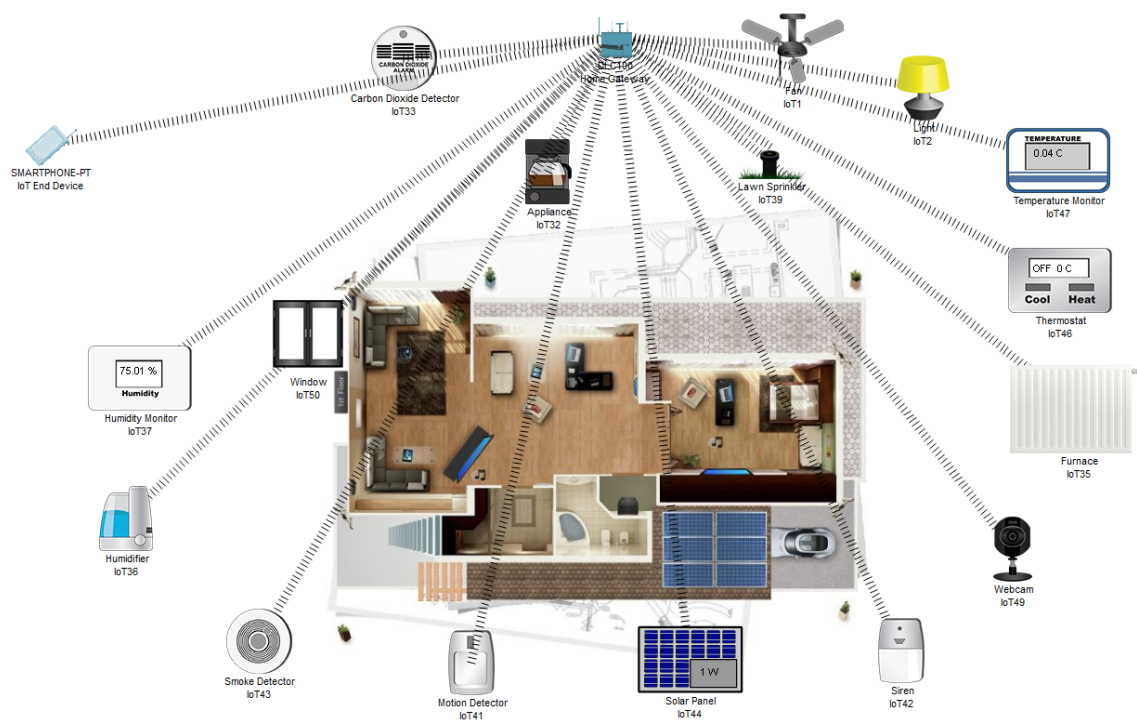


Slika 19. Prikaz pristupa IoT mreži unutar pametne kuće udaljenim putem

Kao što je spomenuto, pristupnik ima glavnu ulogu u dijelu mreže koji je unutar pametne kuće. Na njega se uređaji spajaju žično i bežično, postavljajući IoT poslužitelj kao glavni način spajanja unutar alata Cisco Packet Tracera. Uređaje je potrebno dodati iz alatne trake, a zatim i konfigurirati na pristupnik svaki zasebno. Kao krajnji uređaj u mreži izabran je pametni telefon čija je konfiguracija prikazana na slici 20. Nakon dodavanja uređaja koji su prikazani na slici 21 i njihove konfiguracije te povezivanja s pristupnikom, potrebno je povezati i pametni telefon s pristupnikom kako bi preko istoga mogao pristupiti i vršiti upravljanje uređajima putem širokog skupa akcija.



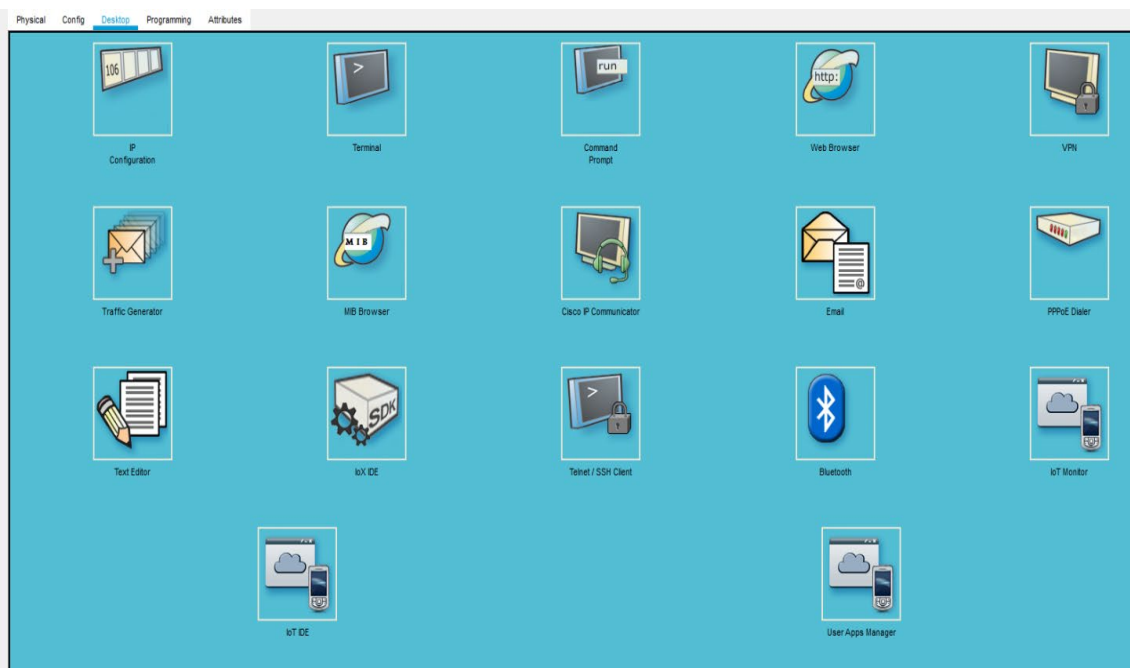
Slika 20. Konfiguracija krajnjeg uređaja za upravljanje



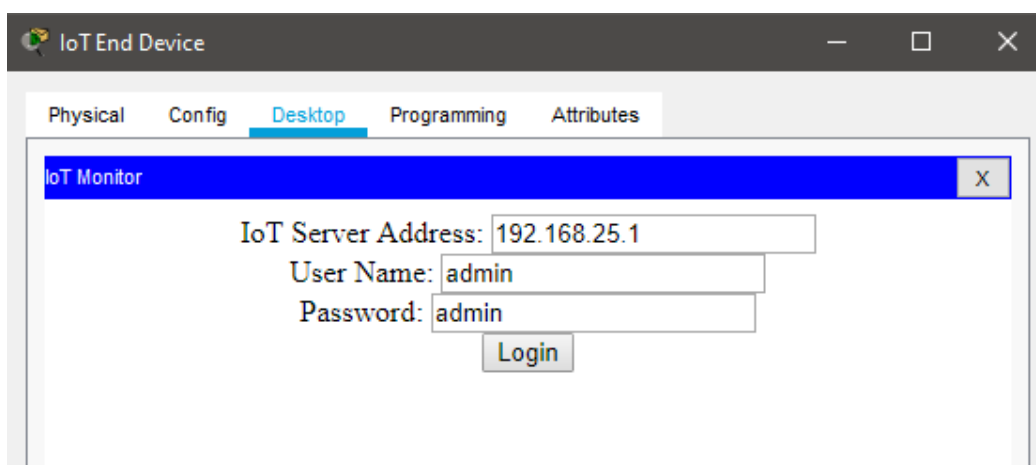
Slika 21. Uređaji unutar IoT mreže spojeni na pristupnik

Pametni telefon, kao i tablet, prijenosno ili stolno računalo ukoliko se koriste kao krajnji

uređaji, ima mnoštvo mogućnosti pristupanja upravljanju mreže. Ima mogućnost konfiguracije IP adresa, izdavanja naredbi kroz terminal, pristup IoT poslužitelju putem web preglednika te IoT aplikacije za nadzor. Može koristiti i spajanja sigurnim putem ostvarujući telnet ili SSH konekciju, uparivati se s drugim uređajima u mreži putem Bluetootha ili pak koristiti virtualnu privatnu mrežu. Sve navedeno prikazano je na slici 22, kao i spajanje na IoT aplikaciju za nadzor pomoću IP adrese poslužitelja i korisničkih podataka na slici 23 čime se omogućuje daljnji pristup i upravljanje.

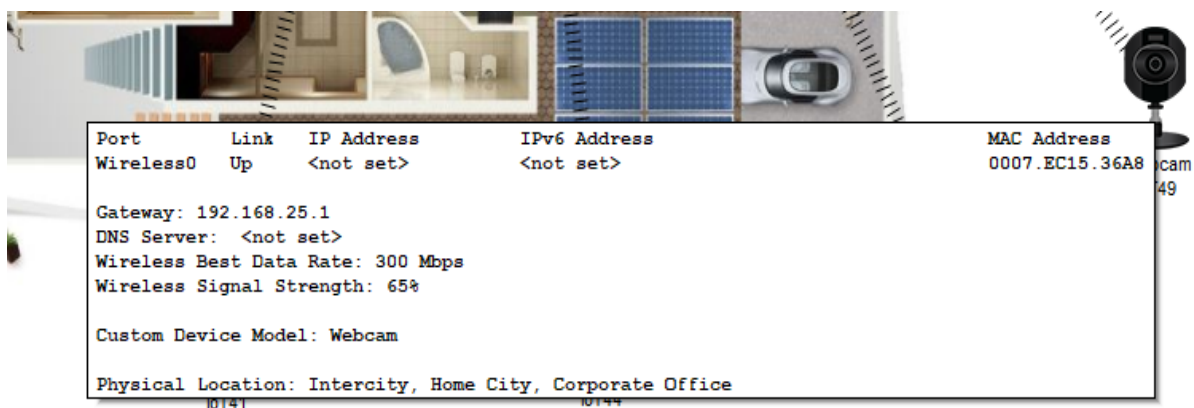


Slika 22. Upravljanje i nadzor putem IoT aplikacije na pametnom telefonu



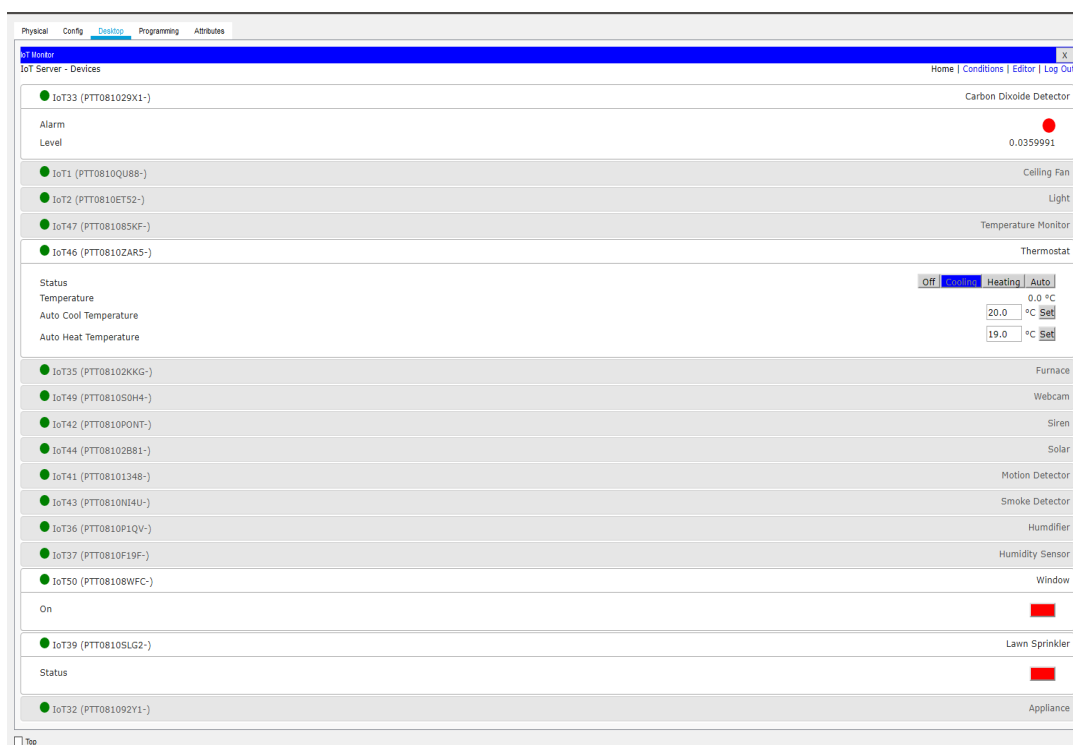
Slika 23. Prijava u IoT aplikaciju za nadzor i upravljanje

Sažetak informacija o postavljenim uređajima moguće je u svakom trenutku vidjeti na logičkom prikazu u sučelju Cisco Packet Tracer alata kao u primjeru na slici 24. Moguće je vidjeti IP i MAC adresu, postoji li aktivna konekcija, IP adresu pristupnika, poslužiteljski server, maksimalnu propusnost i jačinu signala bežične veze te lokaciju i svrhu korištenja uređaja.



Slika 24. Sažetak informacija o uređaju

Nakon što se povežu svi uređaji te tako postanu vidljivi na IoT aplikaciji za nadzor na pametnom telefonu, moguće je upravljati istima kao što je prikazano na slici 25. Za svaki uređaj vidljiva su stanja koja se mogu mijenjati, kao i parametri kod nekih kao što je postavljanje temperature hlađenja ili grijanja na pametnom termostatu.



Slika 25. Povezani uređaji

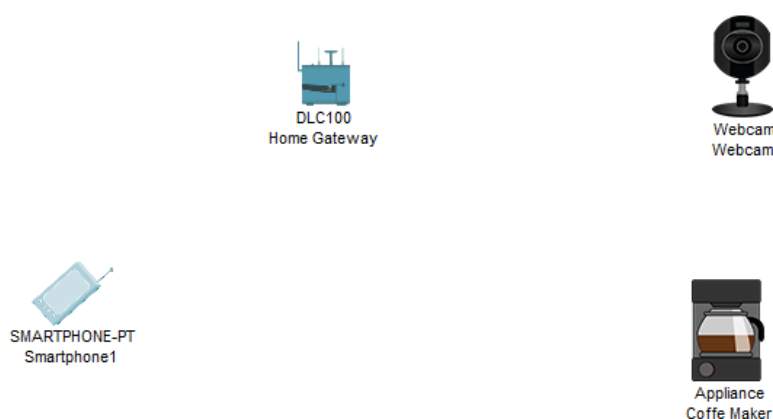
6. Simulacija IoT mreže na primjeru pametne kuće i analiza dobivenih rezultata

Unutar alata Cisco Packet Tracer moguće je simulirati način rada mreže te tako analizirati promjene koje se događaju unutar IoT mreže u okviru pametne kuće. Kroz naredne primjere obradit će se različiti scenariji, a upravljanje, promjena stanja i ponašanje uređaja odvijat će se putem IoT aplikacije za upravljanje udaljenim putem. Scenariji su izabrani kako bi testirali i analizirali odziv sustava, ponašanje sustava pri promjeni određenih parametara te nadzor nad pojedinim elementima sustava. Ključna pitanja simulacije su kako se sustav ponaša u određenim uvjetima, kako reagira na promjenu parametara te kako komponente mreže međusobno komuniciraju i pokreću određene akcije te čime rezultiraju iste. Također, na primjeru će se analizirati i mrežne performanse izabrane IoT mreže.

6.1. Mjerenje mrežnih performansi

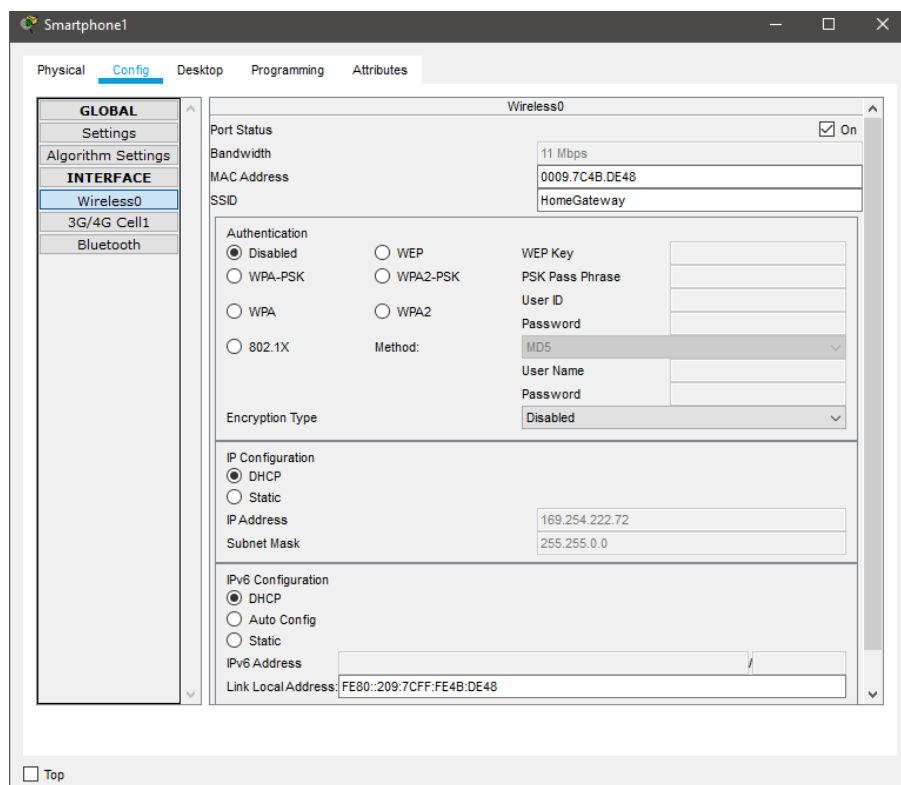
Simulacija predstavlja tehniku u okviru upravljanja i dizajniranja mreža namijenjenu predviđanju performansi mrežnih aplikacija ili sustava prije same izgradnje mreže.

Prvi korak kod izrade mreže je sama vizualizacija i izbor mrežnih komponenti. Na slici 26 prikazane su izabrane mrežne komponente IoT mreže na pozadini alata Cisco Packet Tracer. Navedena mreža se sastoji od pristupnika, korisničkog pametnog telefona, *web* kamere te aparata za kavu.



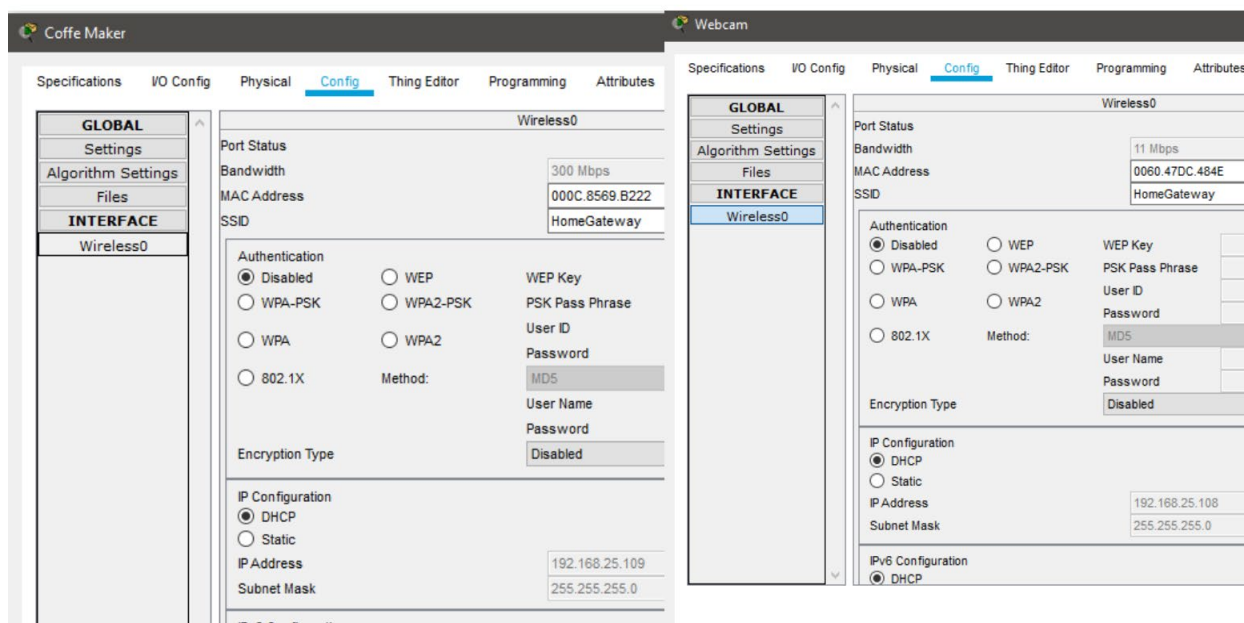
Slika 26. Izabrane mrežne komponente

Korištenjem opcije povezivanja, uređaji se povezuju na pristupnik bežičnim putem. U svrhu uspostavljanja komunikacije, svakom uređaju se mora dodijeliti *default gateway*, IP adresu te masku pod mreže. Također, adresiranje se može obaviti na više načina. U ovom primjeru koristit će se dinamički način (DHCP) gdje sam uređaj šalje zahtjev pri čemu mu se automatski dodjeljuje adresa. Taj zahtjev uređaj šalje pristupniku koji dodjeljuje adresu. Na slici 27 prikazan je dinamički način adresiranja za korisnički pametni telefon.



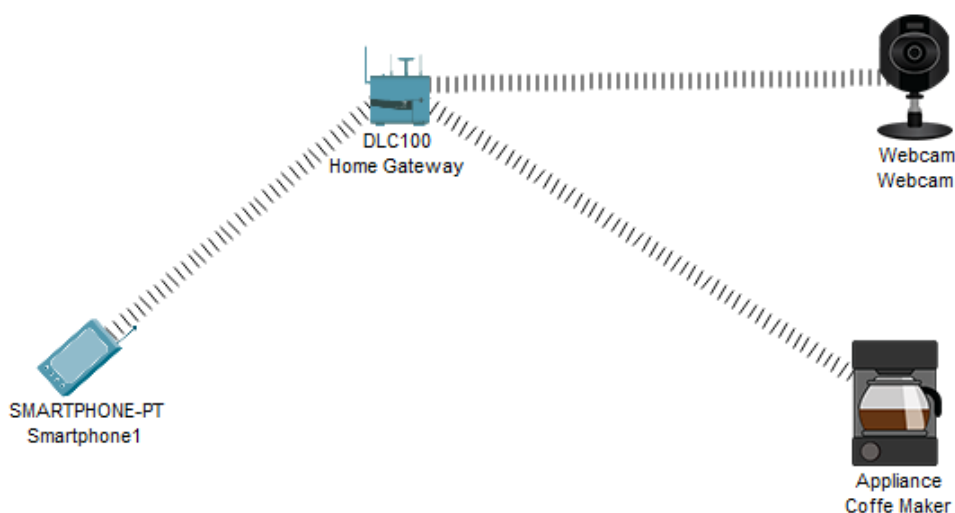
Slika 27. Dinamički način adresiranja

Krajnji uređaj, u ovom slučaju korisnički pametni telefon, mora se konfigurirati kako bi bio bežično spojen na pristupnik. Pri tome se podrazumijeva aktivacija bežičnog modula koji osigurava da se uređaj može spojiti na bežičnu 2.4GHz mrežu. Nadalje, potrebno je i ostalim uređajima u mreži dodijeliti odgovarajuće adrese, što je prikazano na slici 28.



Slika 28. Adresiranje *web* kamere i aparata za kavu

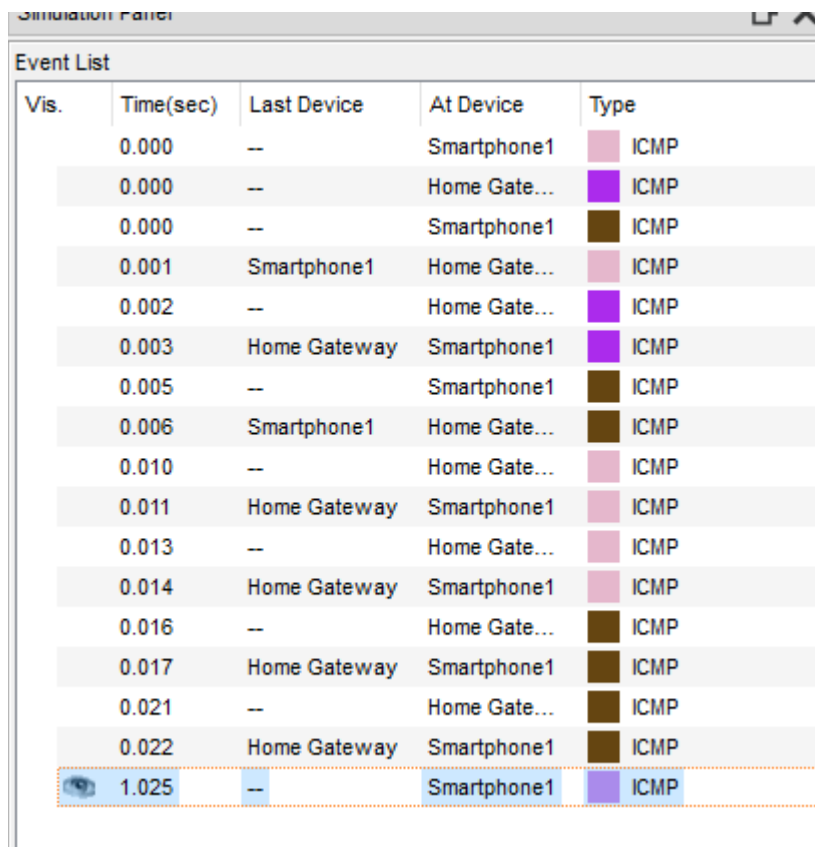
Kako bi se uspješno povezali navedeni uređaji na pristupnu točku, u izborniku je potrebno odabrati bežičnu mrežu te upisati isti SSID koji ima pristupnik. Nakon obavljanja svih navedenih radnji, dobije se jednostavna IoT mreža prikazana na slici 29.



Slika 29. Konačan prikaz IoT mreže

Sve do sada navedeno napravljeno je u *realtime* opciji unutar alata. Kako bi se kreirao scenarij slanja paketa od korisnikovog pametnog telefona prema pristupniku, potrebno je

izabrati simulacijski način rada. Nakon odabira istoga, vidljiva postaje lista događaja, vidljiva na slici 30, koja je zapravo vremenski raspoređen prikaz slanja paketa od izvorišta do odredišta.

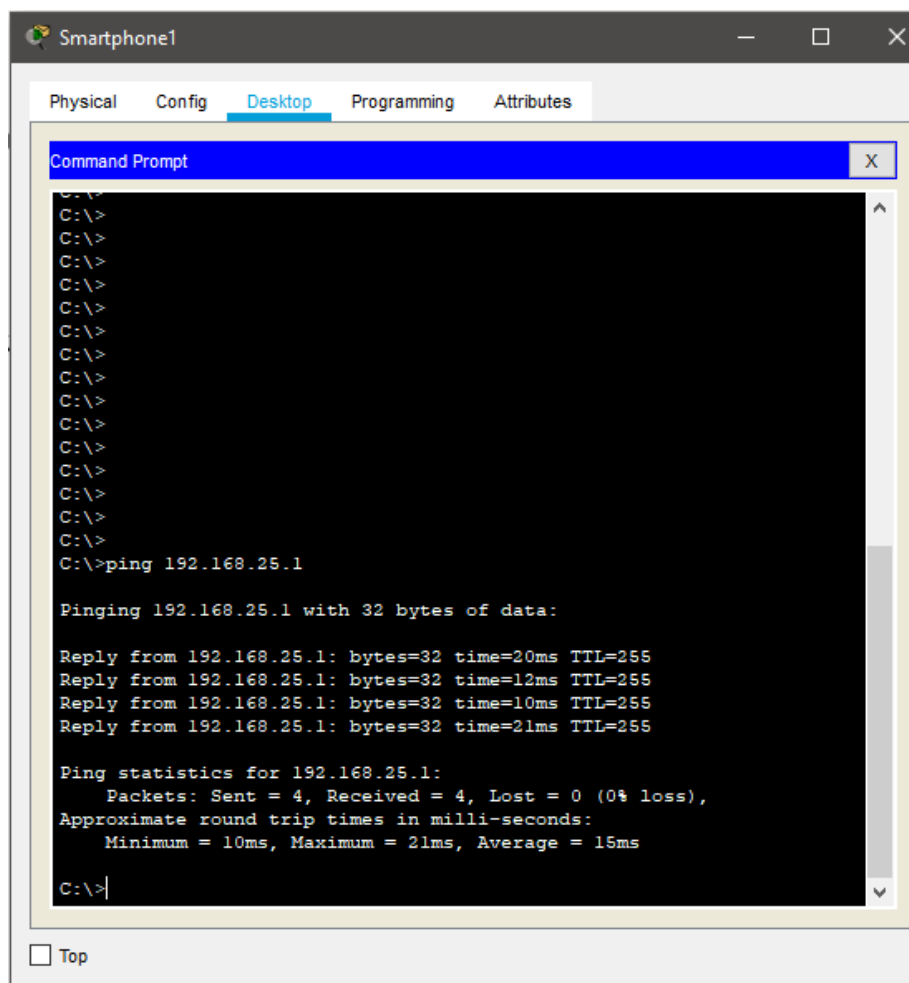


Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Smartphone1	ICMP
	0.000	--	Home Gate...	ICMP
	0.000	--	Smartphone1	ICMP
	0.001	Smartphone1	Home Gate...	ICMP
	0.002	--	Home Gate...	ICMP
	0.003	Home Gateway	Smartphone1	ICMP
	0.005	--	Smartphone1	ICMP
	0.006	Smartphone1	Home Gate...	ICMP
	0.010	--	Home Gate...	ICMP
	0.011	Home Gateway	Smartphone1	ICMP
	0.013	--	Home Gate...	ICMP
	0.014	Home Gateway	Smartphone1	ICMP
	0.016	--	Home Gate...	ICMP
	0.017	Home Gateway	Smartphone1	ICMP
	0.021	--	Home Gate...	ICMP
	0.022	Home Gateway	Smartphone1	ICMP
	1.025	--	Smartphone1	ICMP

Slika 30. Prikaz liste događaja

Između svih komponenata unutar mreže trebala bi biti uspostavljena veza na temelju postavljenih adresa. Provjera uspješne komunikacije, odnosno ispravnosti mreže, može se provjeriti putem IoT aplikacije na samom korisničkom pametnom telefonu. Potrebno je otvoriti naredbeni redak te naredbom ping poslati ICMP zahtjev prema zadanoj adresi odredišta. Ukoliko odredište uspješno primi paket, utvrđuje se kako je veza uspostavljena. Također, samo vrijeme odziva ukazuje na eventualne poteškoće u mreži.

Na slici 31 prikazano je testiranje komunikacije između korisnikovog pametnog telefona i pristupnika tako što je u naredbenom retku unesena naredba ping te IP adresa pristupnika.



Slika 31. Korištenje naredbe ping unutar naredbenog retka i rezultati testiranja

Na slici iznad utvrđena je uspješna komunikacija između uređaja slanjem četiri paketa koja su uspješno zaprimljena. Također, prikazane su performanse mreže kao što je prosječno, najmanje i najveće kašnjenje. Tako prosječno kašnjenje iznosi 15 milisekundi, najmanje 10, a najveće 21 milisekundu.

Nadalje, testirat će se i je li uspostavljena veza između pametnog telefona i aparata za kavu. Na listi događaja prilikom izvođenja naredbe ping vidljivo je slanje ICMP zahtjeva od strane izvorišta (pametnog telefona) prema odredištu (aparat za kavu) putem pristupnika, kao što je i prikazano na slici 32.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.009	--	Smartphone1	ICMP
	0.010	Smartphone1	Home Gate...	ICMP
	0.012	--	Home Gate...	ICMP
	0.013	Home Gateway	Smartphone1	ICMP
	0.013	Home Gateway	Coffe Maker	ICMP
	0.014	--	Coffe Maker	ICMP
	0.015	Coffe Maker	Home Gate...	ICMP
	0.017	--	Home Gate...	ICMP
	0.018	Home Gateway	Smartphone1	ICMP
	0.018	Home Gateway	Coffe Maker	ICMP
	0.020	--	Home Gate...	ICMP
	0.021	Home Gateway	Smartphone1	ICMP
	0.021	Home Gateway	Coffe Maker	ICMP
	0.023	--	Coffe Maker	ICMP
	0.024	Coffe Maker	Home Gate...	ICMP

Slika 32. Lista događaja drugog testiranja komunikacije

Gubitak paketa i kašnjenje prilikom komunikacije između dvije navedene komponente mreže vidljivo je na slici 33.

```

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.25.109

Pinging 192.168.25.109 with 32 bytes of data:

Reply from 192.168.25.109: bytes=32 time=46ms TTL=255
Reply from 192.168.25.109: bytes=32 time=15ms TTL=255
Reply from 192.168.25.109: bytes=32 time=18ms TTL=255
Reply from 192.168.25.109: bytes=32 time=20ms TTL=255

Ping statistics for 192.168.25.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 46ms, Average = 24ms

C:\>

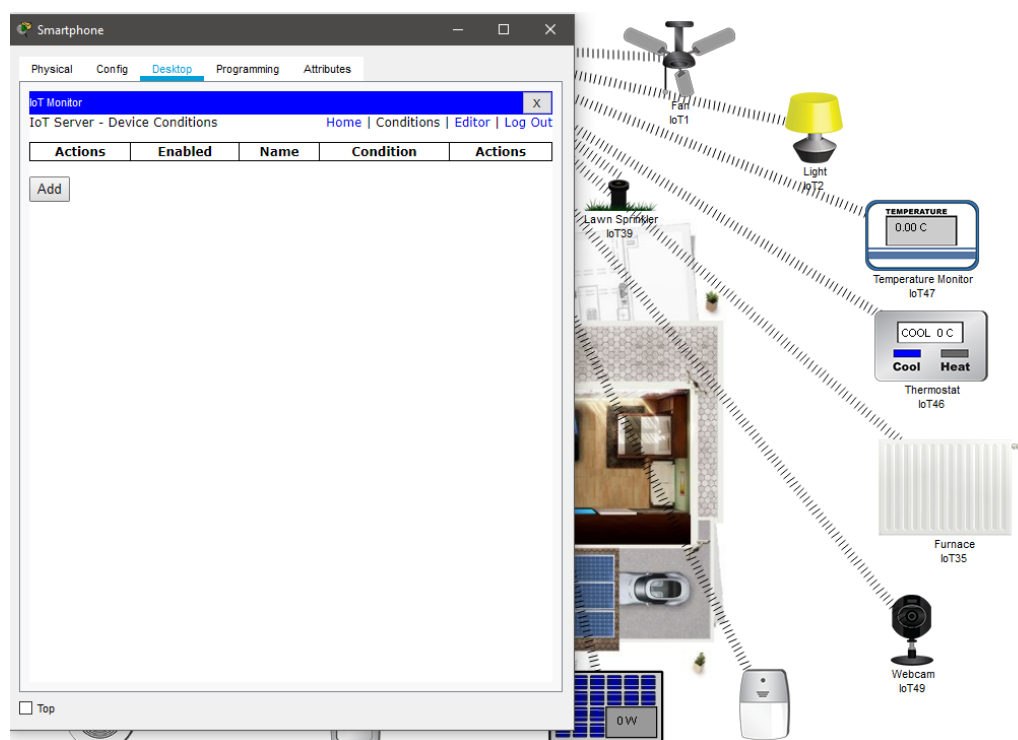
```

Slika 33. Rezultati testiranja veze

Kao što je vidljivo sa slike, uspješno su poslana četiri ICMP paketa te su isti zaprimljeni. Najveće kašnjenje iznosi 46 milisekundi, najmanje 15, a prosječno 24 milisekundi.

6.2. Praćenje i mjerenje parametara unutar IoT mreže

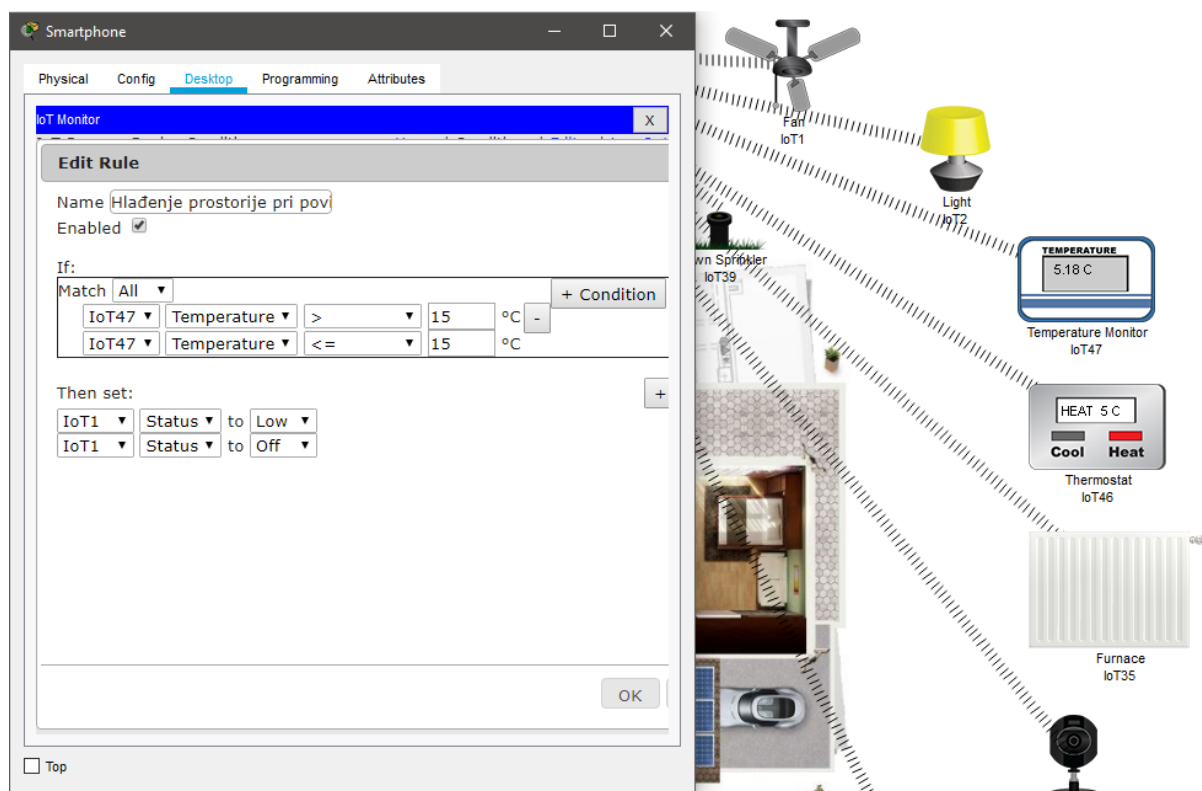
U sljedećem slučaju razmatra se vrijeme odziva sustava temeljeno na promjeni parametra temperature prostorije pametne kuće. Parametar temperature postavljen je na 0 Celzijevih stupnjeva, kao što je prikazano na slici 36 gdje pametni termostat spojen na pristupnik bežičnim putem prikazuje navedenu temperaturu na zaslonu. Cilj je testirati kako će sustav reagirati pod unaprijed određenim pravilima pri promjeni parametara temperature. Izabrane komponente mreže u ovom slučaju su pametni termostat, pametni ventilator i senzor za nadzor temperature. Slika 34 prikazuje komponente IoT mreže te IoT aplikaciju na pametnom telefonu s deaktiviranim komponentama. U ovom primjeru koristit će se mogućnost kreiranja i primjene pravila koju omogućuje IoT aplikacija na pametnom uređaju. Kreiranje pravila podrazumijeva postavljanje „što ako“ scenarija gdje se kasnije nastoji pokrenuti događaj koji će promijeniti stanje unutar sustava kako bi se moglo analizirati zašto je došlo do promjene stanja i na koji način.



Slika 34. IoT aplikacija na pametnom telefonu i izabrane komponente mreže

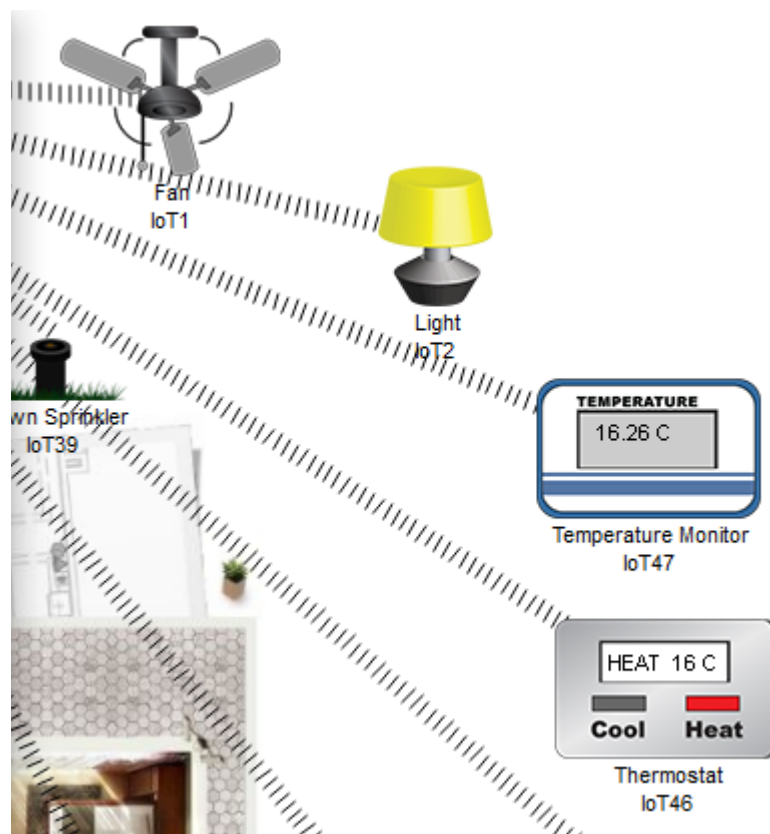
Dodavanjem pravila prikazanih na slici 35 određuje se scenarij u kojem uređaji unutar IoT mreže reagiraju prema postavljenim pravilima ukoliko dođe do događaja koji će aktivirati isto. Senzoru za nadzor temperature kreirana su dva „što ako“ pravila. Ovo testiranje sustava odgovara na pitanja što ako se, prema prvom pravilu, na senzoru za nadzor temperature očita

temperatura veća od 15 Celzijevih stupnjeva, a prema drugom pravilu, što ako je niža ili jednaka istoj vrijednosti. Pretpostavka je, kako je i postavljeno u „što ako“ pravilima, da ako se pojavi događaj koji će zadovoljiti uvjete prvog pravila i promijeniti parametar temperature više od pravilom propisane vrijednosti, sustav mora reagirati paljenjem pametnog ventilatora. U takvom stanju sustav se mora zadržati sve dok pametni ventilator svojim djelovanjem ne spusti vrijednost parametra temperature na onu definiranu drugim pravilom. Ukoliko se takav događaj ostvari, sustav mora reagirati gašenjem pametnog ventilatora.



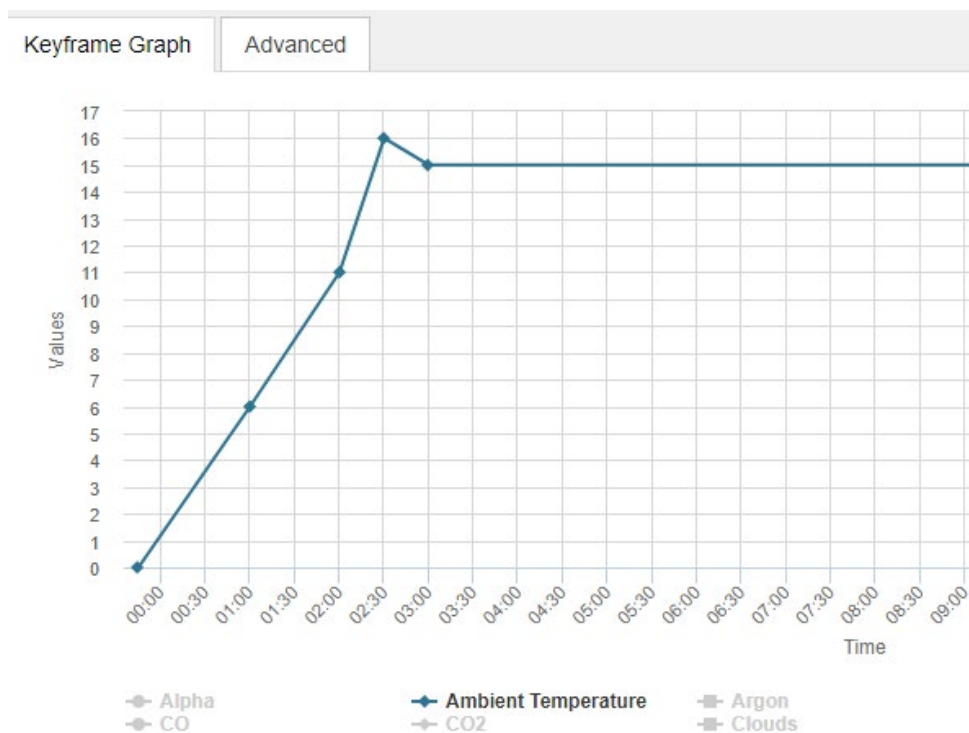
Slika 35. Kreiranje pravila

Na temelju mogućnosti alata pokrenuto je zagrijavanje prostorije paljenjem grijanja prostorije na pametnom termostatu. Nakon određenog vremenskog razdoblja te nakon što je unutar prostorije temperatura prešla 15 Celzijevih stupnjeva, kao što je vidljivo na slici 36, a što je očitano na senzoru za nadzor temperature, sustav je reagirao prema zadanim pravilima u te uključio pametni ventilator kako bi vratio parametar temperature unutar prostorije na željenu vrijednost. Rezultat ovog testiranja je točna i pravovremena reakcija na promjenu parametra temperature te uspješno provedena prethodno postavljena pravila „što ako“.



Slika 36. Vrijednosti nakon promjene parametara

Ukupno praćenje i mjerenje parametara unutar mreže provedeno je u vremenskom razdoblju od četiri sata. Na slici 37 prikazan je graf unutar alata Cisco Packet Tracer koji opisuje promjenu parametra temperature kroz navedeni period.



Slika 37. Graf promjene parametra temperature

U ovom testiranju pokazano je kako je unutar alata moguće pratiti i mjeriti vrijednosti parametara, kao i ponašanje sustava u vidu reakcije na pojedine događaje te vrijeme odziva sustava. Komponentama mreže je moguće manipulirati u vidu postavljanja pravila „što ako“ prema kojima iste moraju reagirati te uzrokovati promjenu parametara u određenom trenutku. To upravo opisuje i samu svrhu pametnih kuća jer automatizacijom svakodnevnih procesa te mogućnošću praćenja i promjene parametara udaljenim putem značajno se olakšava život u svakodnevici te se teži za sličnim rješenjima.

6.3. Diskusija rezultata istraživanja

U ovom poglavlju provedena je simulacija IoT mreže pametne kuće korištenjem alata Cisco Packet Tracer unutar kojeg je pokazano kako se komponente mreže mogu praktično implementirati i konfiguirati. Prikazane mogućnosti kontrole, nadzora i upravljanja dodatno su pokazale jednostavnost korištenja, mogućnosti automatizacije svakodnevnih procesa te pouzdanost ovakve vrste mreže. Simulacije i rezultati ukazuju i na dobre performanse mreže, s obzirom da su se u ovome radu primjeri temeljili na bežičnoj lokalnoj mreži koja je sama po sebi fleksibilna, povoljna za instalaciju te jednostavna za korištenje. Dodatnu prednost predstavlja i mogućnost izgradnje različitih topologija mreže, kao i simuliranje različitih

scenarija, što daje bolji uvid potencijalnim budućnim korisnicima IoT mreže. Ukratko, mogućnost stvaranja sustava s gotovo neograničenim brojem uređaja zapravo opisuje samu ideju IoT mreže kakvom će postati u budućnosti.

IoT mreža nudi širok spektar mogućnosti u vidu povezivanja uređaja, a u ovom slučaju pokazalo se kako se spajanjem na bežičnu lokalnu mrežu postižu dobre performanse mreže, tj. parametri minimalnog, maksimalnog i prosječnog kašnjenja su zadovoljavajući, dok je gubitak paketa također minimalan. Navedeno predstavlja veoma bitnu karakteristiku mreže s obzirom na složenost procesa koje korisnici obavljaju. Osobito je bitno imati takve karakteristike iz razloga što je u okruženju pametne kuće vrlo važna pravovremena i točna reakcija sustava na određeni događaj u mreži.

IoT aplikacija na korisničkom krajnjem uređaju, a koja je opisana u ovom radu, također predstavlja bitan čimbenik kod budućih korisnika. Ono što može doprinijeti povećanju implementacije ovakve vrste mreže u korisničkim domovima je prikazana jednostavnost korištenja, mogućnost udaljenog pristupa te brojne mogućnosti nadzora i upravljanja, što predstavlja također jedan od ključnih interesa sa korisnikovog stajališta.

7. Zaključak

IoT mreža unutar svih područja u kojima je zastupljena, a osobito u okruženju pametne kuće dovodi do smanjivanja potrebe za ljudskom intervencijom u određenim zadacima svakodnevne, pri tom olakšavajući brojne aktivnosti koje korisnik provodi. Iz tog razloga, automatski se javlja i veća produktivnost korisnika zbog fokusa na ono što je bitno. IoT mreža učinkovito upravlja operacijama, učinkovito koristi resurse i čini aktivnosti isplativima. Također, poboljšava brojne usluge te omogućuje širok spektar primjene te se svakodnevno razvija u povoljnom smjeru. Unutar okvira pametne kuće omogućuje upravljanje svim uređajima s jednog mjesta, bilo to s udaljenosti ili iz doma. IoT je izrazito fleksibilan za nove uređaje za implementaciju, povećava sigurnost unutar pametne kuće te povećava energetske učinkovitost. S druge strane, IoT se još uvijek oslanja na ponekad nepouzdan mreže zbog svojih ograničenih resursa i dinamičkih topologija. Održavanje stalne dostupnosti uređaja i pouzdanost komunikacije ključni su čimbenici koji bi garantirali stalan i pouzdan protok podataka.

Cilj ovog diplomskog rada bio je simulirati IoT mrežu unutar pametne kuće. Rezultat je pokazao da se uređajima može upravljati i nadzirati pomoću uređaja krajnjeg korisnika te da su performanse mreže zadovoljavajuće. Cisco Packet Tracer alat pruža razne mogućnosti koje simulaciju čine jednostavnom. Rezultati dokazuju da postoji mogućnost primjene ovog modela u stvarnom životu te da se IoT koncept se može primijeniti u raznim domenama. Za simulaciju pametne kuće korištena je najnovija verzija alata jer uključuje brojne IoT uređaje. Korištena je IoT aplikacija za kućnu automatizaciju i analizirani su pametni uređaji koji služe za kontrolu i nadzor. Također, analizirane su mrežne performanse

Simulacije su se također fokusirale na parametre za praćenje temperature prostorije mjerene senzorima te nadzora i kontrole elemenata pametne kuće. Na temelju navedenog i ostalih uređaja unutar mreže, prikazane su funkcionalnosti proizašle iz međusobne povezanosti i razmjene podataka među istima te kasnija točna i pravovremena reakcija ovisno o događaju. Također, opisane su mogućnosti samih uređaja, način konfiguracije istih unutar mreže pametne kuće, načini povezivanja na pristupnik, kao i stanja u kojima se uređaji mogu naći. Stanjima se može upravljati tako što se unaprijed postave određena pravila te se tako može analizirati reakcija mreže kada se dogodi promjena određenih parametara.

Literatura

- [1] Patel K, Patel M. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future. International Journal of Engineering Science and Computing. 2016 ; 6(5) : 6122-6131.
- [2] Oracle portal. Preuzeto sa <https://www.oracle.com/internet-of-things/what-is-iot/> [Pristupljeno: kolovoz 2021.]
- [3] Portal IT transition. Preuzeto sa <https://www.itransition.com/blog/iot-history> [Pristupljeno: kolovoz 2021.]
- [4] Cisco. The Internet of Things - How the next evolution of the Internet is changing everything. Preuzeto sa: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Pristupljeno: kolovoz 2021.]
- [5] Sethi P, Sarangi S. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. 2017; 2-4.
- [6] Lombardi M, Pascale F, Santaniello D. Internet of Things: A General Overview between Architectures, Protocols and Applications. MDPI. 2021; 12(87): 5-7.
- [7] Sankar S. Introduction to Internet of Things. Site VIT. 2016; 3
- [8] Research gate portal. Preuzeto sa: https://www.researchgate.net/figure/IoT-posrednički-sofтвер-architecture_fig1_254004296 [Pristupljeno: kolovoz 2021.]
- [9] Portal altexsoft. Preuzeto sa: <https://www.altexsoft.com/blog/iot-architecture-layers-components/> [Pristupljeno: kolovoz 2021.]
- [10] Šumiga I, Kolarek F, Srpak D. Inteligentni sustavi za pametnu kuću. Tehnički glasnik. 2014; 8(4): 451-456.
- [11] Gartner. Preuzeto sa: <https://www.gartner.com/newsroom/id/2839717> [Pristupljeno: studeni 2020.]
- [12] Deloitte: The smart factory. Preuzeto sa: https://www2.deloitte.com/content/dam/insights/us/articles/4051_The-smart-factory/DUP_The-smart-factory.pdf [Pristupljeno: kolovoz 2021.]
- [13] Hedge, S. Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges. International Journal of Advanced Networking & Applications (IJANA). 2016; 477-481.
- [14] Portal Comparitech. Preuzeto sa: <https://www.comparitech.com/internet-providers/iot-statistics/> [Pristupljeno: kolovoz 2021.]

- [15] Rattletech portal. Preuzeto sa: <https://www.rattletech.com/4-main-components-smart-home-building-solution/> [Pristupljeno kolovoz 2021.]
- [16] Mouha, R. Internet of Things (IoT). Journal of Data Analysis and Information Processing. 2021; 9(2): 10-42
- [17] Portal Tech beacon. Preuzeto sa: <https://techbeacon.com/app-dev-testing/top-6-programming-languages-iot-projects> [Pristupljeno: kolovoz 2021.]
- [18] Udoh I, Kontonya G. Developing IoT applications: Challenges and Frameworks. IET Cyber-Physical Systems. 2017; 4(2): 1-11
- [19] Electronic Design portal. Preuzeto sa: <https://www.electronicdesign.com/technologies/iot/article/21798493/understanding-the-protocols-behind-the-internet-of-things> [Pristupljeno: kolovoz 2021.]
- [20] Biswajeon M, Kertesz, A. The Use of MQTT in M2M and IoT Systems: A Survey. IEEE Access. 2020; 8: 71-75
- [21] Behrtech portal. Preuzeto sa: <https://behrtech.com/blog/mqtt-in-the-iot-architecture/> [Pristupljeno: kolovoz 2021.]
- [22] Malik M, McAteer I, Hannay P, Firdous N, Baig Z. XMPP architecture and security challenges in an IoT ecosystem. Information Security Management Conference. 2018; 62-73
- [23] Portal Object management group. Preuzeto sa: <https://www.omg.org/intro/DDS.pdf> [Pristupljeno: kolovoz 2021.]
- [24] Researchgate portal. Preuzeto sa: https://www.researchgate.net/figure/Essential-DDS-architecture_fig1_261486849 [Pristupljeno: kolovoz 2021.]
- [25] Smartsbear portal. Preuzeto sa: <https://support.smartbear.com/readyapi/docs/testing/amqp.html> [Pristupljeno: kolovoz 2021.]
- [26] Researchgate portal. Preuzeto sa: https://www.researchgate.net/figure/IoT-Communication-technologies-Source-White-Paper-What-the-Internet-of-Things-IoT_fig6_317402215/download [Pristupljeno: kolovoz 2021.]
- [27] Portal Gyanoholic. Preuzeto sa: <http://www.gyanoholic.com/blog/what-is-nfc-technology> [Pristupljeno: kolovoz 2021.]
- [28] Ray P. A survey on Internet of Things architectures. Journal of King Saud University – Computer and Information Sciences. 2018;30:291–319. Preuzeto sa sustava Merlin [Pristupljeno: studeni 2018.]
- [29] Trend micro portal. Preuzeto sa: <https://www.trendmicro.com/vinfo/us/security/definition/lorawan> [Pristupljeno: kolovoz 2021.]

[30] Matković P. Norme i protokoli za automatizaciju kućanstva, Diplomski rad. Sveučilište u Zagrebu. Fakultet elektrotehnike i računarstva. Zagreb. 2013.

[31] Tutorial web portal. Preuzeto sa: <https://www.tutorialsworld.com/networking/wireless-networks/computer-network-planning-and-design.htm> [Pristupljeno: kolovoz 2021.]

[32] Firardi A. IoT Simulations with Cisco Packet Tracer. Diplomski rad. Helsinki Metropolia University of Applied Sciences. Engineering Information Technology. Helsinki. 2018.

Popis kratica

IoT (Internet of things) Internet stvari

TCP (Transmission Call Protocol) protokol za kontrolu prijenosa podataka

IP (Internet Protocol) mrežni protokol za prijenos podataka

RFID (Radio-frequency identification) tehnologija koja koristi radio frekvenciju za razmjenu informacija

LAN (Local Area Network) lokalna računalna mreža

NFC (Near-field Communication) kratkodometna bežična tehnologija

SoA (Service-oriented architecture) uslužno orijentirana arhitektura

API (Application programming interface) aplikacijsko programsko sučelje

QoS (Quality of service) kvaliteta usluge

VoIP (Voice over IP) komunikacijska tehnologija koja omogućava prijenos glasovne komunikacije preko internetske mreže

DNS (Domain Name System) hijerarhijski distribuirani sustav imenovanja

M2M (Machine to Machine) komunikacija strojeva

TLS (Transport Layer Security) kriptografski protokol koji omogućuje sigurnu komunikaciju

PAN (Personal Area Network) osobna računalna mreža

WAN (Wide area network) mreža širokog područja

IEEE (Institute of Electrical and Electronics Engineers) međunarodna neprofitna profesionalna organizacija za uznapredovanje tehnologije vezane sa električnom energijom

WEP (Wired Equivalent Privacy) algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža

WPA (Wi-Fi Protected Access) algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža

SBC (Single-board computer) funkcionalno računalo na jednoj tiskanoj ploči

SSID (Service Set Identifier) identifikator postavljenog servisa

DHCP (Dynamic Host Configuration Protocol) mrežni protokol za dodjeljivanje IP adresa i ostalih mrežnih postavki

MAC (Media Access Control Address) adresa za kontrolu pristupa medijima

SSH (Secure Shell) mrežni protokol koji omogućuje uspostavu sigurnog komunikacijskog kanala

Popis slika

Slika 1. Troslojna i peteroslojna arhitektura IoT-a	6
Slika 2. Uslužno orijentirana arhitektura IoT-a	8
Slika 3. Arhitektura posredničkog softvera	9
Slika 4. Ključni gradivni elementi arhitekture IoT	10
Slika 5. Funkcionalnosti pametne kuće	13
Slika 6. Prijelaz s tradicionalnog lanca opskrbe na digitalnu mrežu opskrbe	15
Slika 7. E2E IoT arhitektura	20
Slika 8. IoT cloud <i>back-end</i> arhitektura	24
Slika 9. Dijagram slijeda MQTT u arhitekturi IoT	28
Slika 10. XMPP protokol	29
Slika 11. Arhitektura DDS protokola	30
Slika 12. Arhitektura AMQP protokola	31
Slika 13. Topologija Zigbee mreže	36
Slika 14. Grafičko sučelje alata Cisco packet tracer	39
Slika 15. Mogućnosti dodavanja elemenata pametne kuće u okviru alata	40
Slika 16. Konfiguracija uređaja	41
Slika 17. Napredne mogućnosti konfiguracije uređaja	41
Slika 18. Konfiguracija povezivanja s bežičnom mrežom	42
Slika 19. Prikaz pristupa IoT mreži unutar pametne kuće udaljenim putem	43
Slika 20. Konfiguracija krajnjeg uređaja za upravljanje	44
Slika 21. Uređaji unutar IoT mreže spojeni na pristupnik	44
Slika 22. Upravljanje i nadzor putem IoT aplikacije na pametnom telefonu	45
Slika 23. Prijava u IoT aplikaciju za nadzor i upravljanje	45
Slika 24. Sažetak informacija o uređaju	46
Slika 25. Povezani uređaji	46
Slika 26. Izabrane mrežne komponente	47
Slika 27. Dinamički način adresiranja	48
Slika 28. Adresiranje <i>web</i> kamere i aparata za kavu	49
Slika 29. Konačan prikaz IoT mreže	49
Slika 30. Prikaz liste događaja	50
Slika 31. Korištenje naredbe ping unutar naredbenog retka i rezultati testiranja	51

Slika 32. Lista događaja drugog testiranja komunikacije	52
Slika 33. Rezultati testiranja veze	52
Slika 34. IoT aplikacija na pametnom telefonu i izabrane komponente mreže	53
Slika 35. Kreiranje pravila	54
Slika 36. Vrijednosti nakon promjene parametara	55
Slika 37. Graf promjene parametra temperature	56

Popis tablica

Tablica 1. Broj povezanih uređaja od 2003. do 2020.	5
Tablica 2. Karakteristike komunikacijskih tehnologija u IoT-u	32

Popis grafikona

Grafikon 1. Broj povezanih uređaja u narednim godinama izražen u milijardama	18
Grafikon 2. Broj pametnih kuća izražen u milijunima	19



Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj _____ diplomski rad
isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na
objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz
necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj
visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu _____ diplomskog rada
pod naslovom **Simulacija rada IoT mreže primjenom programske podrške Cisco**

Packet Tracer

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom
repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 3.9.2021. _____

Student/ica:

Ivan Arapović
(potpis)